

A CLOUD BUSINESS INTELLIGENCE SECURITY  
EVALUATION FRAMEWORK FOR SMALL AND  
MEDIUM ENTERPRISES

by

MOSES MOYO

*(Student number: 46351574)*

Submitted in accordance with the requirements

for the degree of

DOCTOR OF PHILOSOPHY

in

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR MARIANNE LOOCK

28 SEPTEMBER 2021

## **DECLARATION**

I hereby declare that this thesis: A CLOUD BUSINESS INTELLIGENCE SECURITY EVALUATION FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES, submitted for evaluation towards the requirements of the subject: INFORMATION SYSTEMS, as part of the DOCTOR OF PHILOSOPHY qualification at the University of SOUTH AFRICA, is my original work and has not previously been submitted to any other institution of higher learning or subject for evaluation. All sources used or quoted in this document are indicated and acknowledged in a comprehensive list of references.

\_\_\_\_\_  \_\_\_\_\_

SIGNATURE

*MOSES MOYO*

\_\_\_\_\_28 SEPTEMBER 2021\_\_\_\_\_

DATE

## **FULL DISCLOSURE INFORMATION**

### **i. Ethical Clearance:**

The research study reported in this thesis received ethical clearance (*ERC Reference #: 014/MM/2016/CSET\_SOC*) from UNISA's College of Science, Engineering, and Technology Research and Ethics Committee before the collection of data (*see Appendices A and B for the ethical clearance letters*). Therefore, data collection for this research was conducted following the high ethical principles stipulated in the ethical clearance.

### **ii. Similarity Checking:**

Turnitin was used for similarity check in the final thesis and the digital receipt is available (*see Appendix C*). The percentage of similarity was 10%, no single source had a percentage of five or greater. Although this score may seem to be high, most of the sources point to some of my published articles derived from this study.

### **iii. Professional Editing:**

This thesis was professionally edited by Lianne Hugo. The editing certificate is attached (*see Appendix D*)

### **iv. Literature Referencing:**

The University of South Africa (Cite-it Right) Harvard citation style was applied throughout the thesis. Both in-text citation and the compilation of the final reference list was managed by the Mendeley citation manager. The Mendeley Citation Manager was further used in organising and periodic updating of literature sources in the thesis. The last literature sources were updated on 28 September 2021 before finalising the writing of the thesis.

### **v. Publications**

The following publications were a result of the work reported in this thesis.

- **Peer-reviewed journal**

**Moyo, M. & Loock, M. (2021) Conceptualising a Cloud Business Intelligence Security Evaluation Framework for Small and Medium Enterprises in Small Towns of the Limpopo**

Province, South Africa. *Journal of Information Science and Technology, Data, Knowledge, and Communication. A Special Issue of Information.* (ISSN 2078-2489)

- **Peer-reviewed Book Chapters**

**Moyo, M.** & Loock, M. (2020) Evaluation of cloud business intelligence before adoption: The voice of small business enterprises in a South African township. *Lecture Notes in Business Information Processing.* Van Der Aalst, W., Mylopoulos, J., Rosemann, M., Shaw, M.J., Szyperski, C. (Eds). 17<sup>th</sup> European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS), Dubai, United Arab Emirates. 25 – 26 November 2020, Springer. (ISSN 1865-1348)

**Moyo, M.** & Loock, M. (2019) Small and medium enterprises' understanding of security evaluation of cloud business intelligence systems and challenges. *Information Security, Communications in Computer and Information Science 973:* Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (Eds). 17th International Conference, ISSA 2018 Pretoria, South Africa, 15-16 August 2018, Revised Selected Papers, Springer and Information Security, South Africa.

- **Peer-reviewed conferences proceedings**

**Moyo, M.** & Loock, M. (2019) An Analysis of Small and Medium-Sized Enterprises' Perceptions of Security Evaluation in Cloud Business Intelligence: Van Der Waag-Cowling, N., Leensen, L (Eds). *Proceedings of the 14th International Conference on Cyber Warfare and Security*, Stellenbosch, South Africa 28 February - 01 March 2019. pp 554 – 562. E-Book ISBN: 978-1-912764-12-9 & Book version ISBN: 978-1-912764-11-2.

**Moyo, M.** & Loock, M. (2017) South African small and medium-sized enterprises' reluctance to adopt and use cloud business intelligence systems: A literature review. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).* IEEE Xplore: 16 February 2017.

## **ACKNOWLEDGEMENTS**

First and foremost, I express my unreserved gratitude to my supervisor, Professor Marianne Looock, for her unwavering, continuous support and encouragement throughout my PhD study. I sincerely appreciate her expert support and knowledge in completing the challenging doctoral thesis. Prof. Looock's work ethic and professionalism have been exceptional, and I owe my success to her scholarly guidance. I further thank the UNISA Research Bursary Fund for funding part of this study. Special thanks go to Courage Matobobo and Francis Manzira (my PhD colleagues), Mr Kudakwashe Madzima, Dr Bethel Mutanga, Dr Lawrence Meda, and Mr William Zivanai who spent their precious time proofreading research articles and chapters of the thesis. I extend my gratitude to all the IT-security specialists and SME decision-makers who took part in this study by completing questionnaires and participating in interviews. It would be unjust not to mention my family, who encouraged me throughout the study.

## **DEDICATIONS**

This study is dedicated to my wife, family, and late grandmother.

## **ABSTRACT**

Cloud business intelligence has practical importance in data management and decision-making, but the adoption and use among South African small and medium enterprises remain relatively low compared to large business enterprises. The low uptake persists irrespective of the awareness and acceptance of the benefits of Cloud business intelligence in the business domain. Cloud business intelligence depends on the cloud computing paradigm, which is susceptible to security threats and risks that decision-makers must consider when selecting what applications to use. The major objective of this study was to propose a security evaluation framework for Cloud business intelligence suitable for use by small and medium enterprises in small South African towns. The study utilised the exploratory sequential mixed-method research methodology with decision-makers from five towns in the Limpopo Province. Both qualitative and quantitative methods were used to analyse the data. The findings show that the level of adoption of Cloud business intelligence in the five selected towns was lower than reported in the literature, and decision-makers were eager to adopt and use safe Cloud business intelligence, but this was hindered by their inability to evaluate security in these applications. Factors preventing the adoption of Cloud business intelligence were decision-makers' limited knowledge of the applications and security evaluation, the inability to use industry security frameworks and standards due to their complexities, mistrust of cloud service providers in meeting their obligations when providing agreed services, and lack of security specialists to assist in the evaluation process. Small and medium enterprises used unapproved security evaluation methods, such as relying on friends who were not information technology security specialists. A security evaluation framework and checklists were proposed based on the findings of the study and the best practices of the existing industry frameworks and standards. The proposed security evaluation framework was validated for relevance by information technology security specialists and acceptance by small and medium enterprise decision-makers. The study concluded that the adoption and use of Cloud business intelligence were hindered by the lack of a user-friendly security evaluation framework and limited security evaluation knowledge among decision-makers. Furthermore, the study concluded that the proposed framework and checklists were a relevant solution as they were accepted as useful to assist decision-makers to select appropriate Cloud business intelligence for their enterprises. The main contribution of this study is the proposed security evaluation framework and the checklists for Cloud business intelligence, for use by decision-makers in small and medium enterprises in small South African towns in the Limpopo Province.

**Key terms:** Technology adoption process, Cloud business intelligence, Decision-making, Cloud computing, Operational-use-evaluation, Prior-operational-use evaluation, Security evaluation framework, Security vulnerability, Small and medium enterprises, Software-as-a-Service

## LIST OF TABLES

|  |     |
|--|-----|
| Table 3.2: Determination of suitability of design based on research questions .....          | 82  |
| Table 4.1: Themes and sub-themes on adopting and using Cloud BI.....                         | 103 |
| Table 4.2: Demographic information of SME decision-makers .....                              | 104 |
| Table 4.3: Stages of adoption of Cloud BI for 13 participants.....                           | 106 |
| Table 4.4: Knowledge of benefits of the use of Cloud BI among SMEs .....                     | 111 |
| Table 4.5: Influence of benefits on the recommendation to adopt Cloud BI .....               | 112 |
| Table 4.6: Impact of knowledge and skills in preventing the adoption of Cloud BI .....       | 121 |
| Table 4.8: The importance of decision-makers' knowledge and skills in security evaluation .. | 136 |
| Table 4.9: Perceived usefulness of security framework.....                                   | 152 |
| Table 6.1: Summary evaluation sheet .....  | 230 |
| Table 6.2: Decision-making list .....  | 230 |
| Table 7.1: Relevance of each of the six components of the framework .....                    | 237 |
| Table 7.2: Validating framework concerning traditional frameworks .....                      | 239 |
| Table 7.3: Validation of overall relevance of aspects of the framework .....                 | 240 |
| Table 7.4: Demographic information of acceptance reviewers.....                              | 241 |
| Table 7.5: Educational background of reviewers .....   | 242 |
| Table 7.6: Chi-square test for framework components acceptability on reviewers .....         | 248 |
| Table 8.1: List of research objectives and questions.....                                    | 254 |
| Table AP3.1: Mixed methods designs, characteristics, purpose, and suitability .....          | 332 |
| Table AP4.1: Reliability of the survey questionnaire items used in the QUAN phase.....       | 333 |
| Table AP4.2: Chi-Square test knowledge about and benefits of Cloud BI.....                   | 334 |
| Table AP4.3: Knowledge of strategies in security evaluation in Cloud BI .....                | 334 |
| Table AP4.4: Considerations to be made during security evaluations.....                      | 335 |
| Table AP4.5: Chi-Square test dependence on educational level and security evaluation.....    | 336 |
| Table AP4.6: Challenges of evaluation of Cloud BI among decision-makers.....                 | 336 |
| Table AP7.1: Demographic results of reviewer for relevance validation of the framework ..... | 343 |
| Table AP7.2: Relevance of evaluation activities for framework component.....                 | 344 |



## LIST OF FIGURES

|   |     |
|---|-----|
| Figure 1.1: Thesis layout structure .....   | 14  |
| Figure 2.1: Generalised Cloud BI Architecture.....  | 18  |
| Figure 3.1: Research process.....   | 68  |
| Figure 3.3: Types of IS knowledge derived from a pragmatic research .....                         | 74  |
| Figure 3.4: Inclusion and Exclusion criteria .....  | 88  |
| Figure 3.5: Exploratory sequential mixed-methods data collection and analysis .....               | 89  |
| Figure 3.6: Steps in designing and pilot testing a semi-structured interview .....                | 90  |
| Figure 3.7: Six steps for thematic data analysis .....  | 93  |
| Figure 3.8: Sample of coding for belief .....   | 94  |
| Figure 3.9: The steps in developing a questionnaire .....   | 96  |
| Figure 4.1: Distribution of respondents by the number of employees in SMEs .....                  | 105 |
| Figure 4.2: Impact of cyber breaches on decisions to adopt Cloud BI .....                         | 115 |
| Figure 4.3: Challenges related to CSPs preventing the adoption of Cloud BI.....                   | 118 |
| Figure 4.4: Financial risks due to litigation and loss of services to customers .....             | 119 |
| Figure 4.5: Ratings on the frequency of use of selected tools in evaluating IT solutions.....     | 130 |
| Figure 4.6: Perceived important components of a security framework .....                          | 149 |
| Figure 4.7: Mean scores on perceived components of a security framework .....                     | 149 |
| Figure 6.1: Findings that form the basis of the framework .....                                   | 205 |
| Figure 6.2: Components of security evaluating framework for Cloud BI.....                         | 206 |
| Figure 6.3: Cloud Business Intelligence Security Evaluation Framework for SMEs .....              | 207 |
| Figure 6.4: An expanded security evaluation framework for Cloud-BI.....                           | 208 |
| Figure 6.5: Business needs and security requirements for data to be migrated to the cloud .....   | 209 |
| Figure 6.6: Assessing different aspects of Cloud BI .....   | 211 |
| Figure 6.7: Service delivery model assessment.....  | 215 |
| Figure 6.8: Cloud deployment model considerations.....  | 217 |
| Figure 6.9: Cloud service provide assessment and selection .....                                  | 221 |
| Figure 6.10: Financial risks assessment .....   | 226 |
| Figure 6.11: Layout of the evaluation process .....   | 229 |
| Figure 7.1: Ratings of the acceptability of each component of CBISEF by SMEs .....                | 242 |
| Figure 7.2: Ratings of acceptability of Cloud BI security evaluation activities in checklists.... | 243 |

Figure 7.3: Rating of acceptability of checklists aspects .....244

Figure 7.4: Acceptability of language used, length and layout of checklists .....245

Figure 7.5: Acceptability of the proposed framework in implementing traditional security standards and frameworks .....245

Figure 7.6: Overall rating of the acceptability of each aspect of the framework .....246

Figure 7.7: Overall recommendation for acceptability .....247

Table 7.7: Chi-square tests of independence based on the type of reviewers .....249

Figure AP6.1: Checklist 1: Assessing business and data security requirements .....338

Figure AP6.2: Checklist 2: Assessing cloud business intelligence usability .....339

Figure AP6.3: Checklist 3: Assessing service delivery models .....340

Figure AP6.4: Checklist 4: Assessing Cloud deployment models .....340

Figure AP6.5: Checklist 5: Assessing security, trust, reliability and performance of CSP .....341

Figure AP6.6: Checklist 6: Assessing financial risks .....342

## LIST OF ACRONYMS

| ACRONYM       | MEANING  |
|---------------|--|
| BI            | Business Intelligence  |
| CBISEF        | Cloud Business Intelligence Security Evaluation Framework  |
| CIA           | Confidentiality, Integrity and Availability  |
| Cloud BI      | Cloud Business Intelligence  |
| COBIT         | Control Objectives for Information and Related Technologies  |
| CSA           | Cloud Security Alliance  |
| DoIT          | Diffusion of Innovation Theory   |
| ENISA         | European Union Agency for Network and Information Security   |
| ERM           | Enterprise Risk Management   |
| ERP           | Enterprise Resource Planning   |
| HIPAA         | Healthcare Insurance Portability and Accountability Act  |
| IaaS          | Infrastructure-as-a-Service  |
| IS            | Information Systems  |
| ISACA         | Information Systems Audit and Control Association  |
| ISO 70        | International Organization for Standardization 70  |
| ISO/IEC 27000 | International Organization for Standardization and International Electrotechnical Commission 27000 |
| ISO-27001     | International Standards Organisation 27001   |
| ISRMF         | Information Security Risk Management Framework   |
| IT            | Information Technology   |
| MSAM          | Multi-Stage Adoption Model   |
| NIST          | National Institute of Standards and Technology   |
| OUE           | Operational-Use-Evaluation   |
| PaaS          | Platform-as-a-Service  |
| PCI DSS       | Payment Card Industry's Data Security Standard   |
| PDCA          | Plan-Do-Check-Act  |
| PEU           | Perceived Ease-of-Use  |
| POUE          | Prior-Operational Use Evaluation   |
| PU            | Perceived Usefulness   |
| QUAL          | Qualitative  |

| <b>ACRONYM</b> | <b>MEANING</b>                         |
|----------------|--|
| QUAN           | Quantitative                           |
| ROM            | Research Onion Model                   |
| SaaS           | Software-as-a-Service                  |
| SMEs           | Small and Medium Enterprises           |
| UIs            | User interfaces                        |
| UK             | United Kingdom                         |
| VAPT           | Vulnerability Assessment and Pen Tests |

## TABLE OF CONTENTS

|  |      |
|--|------|
| DECLARATION.....   | ii   |
| FULL DISCLOSURE INFORMATION .....                            | iii  |
| ACKNOWLEDGEMENTS .....                                       | v    |
| DEDICATIONS .....  | vi   |
| ABSTRACT .....   | vii  |
| LIST OF TABLES .....   | viii |
| LIST OF FIGURES.....   | ix   |
| LIST OF ACRONYMS.....  | xi   |
| TABLE OF CONTENTS .....                                      | xiii |
| CHAPTER 1 INTRODUCTION TO THE STUDY .....                    | 1    |
| 1.1. Background .....  | 2    |
| 1.2. The problem statement .....                             | 5    |
| 1.3. Purpose of the study .....                              | 6    |
| 1.4. Research objectives and research questions .....        | 7    |
| 1.5. Research focus.....                                     | 9    |
| 1.6. Scope and context of the study.....                     | 9    |
| 1.7. Research methodology .....                              | 9    |
| 1.7.1. Population, sample size and sampling procedures ..... | 10   |
| 1.7.2. Data generation and analysis techniques.....          | 10   |
| 1.8. Contribution of the study.....                          | 10   |
| 1.8.1. Scientific value .....                                | 10   |
| 1.8.2. Business value .....                                  | 11   |
| 1.8.3. Academic community.....                               | 11   |
| 1.9. Benefits of the study.....                              | 12   |

|   |  |           |
|---|--|-----------|
| 1.10.                                   | Definition of the terminology used in the thesis .....                         | 12        |
| 1.11.                                   | The layout of the thesis .....   | 13        |
| 1.12.                                   | Summary .....  | 14        |
| <b>CHAPTER 2 LITERATURE REVIEW.....</b> |  | <b>16</b> |
| 2.1.                                    | Introduction .....   | 17        |
| 2.2.                                    | Definition of cloud business intelligence .....                                | 17        |
| 2.3.                                    | Cloud deployment models.....   | 20        |
| 2.4.                                    | State of adoption of cloud business intelligence .....                         | 22        |
| 2.5.                                    | Factors influencing the adoption of Cloud business intelligence.....           | 22        |
| 2.5.1.                                  | The technology adoption theories .....   | 22        |
| 2.5.2.                                  | Benefits of Cloud business intelligence as enabling factors to adoption .....  | 31        |
| 2.5.3.                                  | Characteristics of small and medium enterprises .....                          | 39        |
| 2.5.4.                                  | Security risk factors in cloud business intelligence.....                      | 41        |
| 2.5.5.                                  | Cloud service providers .....  | 48        |
| 2.5.6.                                  | Financial risks.....   | 49        |
| 2.6.                                    | Strategies used to evaluate cloud business intelligence .....                  | 50        |
| 2.6.1.                                  | Understanding security evaluation in cloud business intelligence .....         | 50        |
| 2.6.2.                                  | Initiatives in cloud business intelligence evaluation before adoption .....    | 52        |
| 2.7.                                    | Security evaluation challenges for cloud business intelligence .....           | 57        |
| 2.7.1.                                  | Knowledge of security evaluation in cloud business intelligence.....           | 58        |
| 2.7.2.                                  | The complexity of industry security evaluation framework and standards.....    | 59        |
| 2.7.3.                                  | Lack of information on cloud business intelligence from service providers..... | 59        |
| 2.8.                                    | Security evaluation frameworks for cloud business intelligence .....           | 60        |
| 2.8.1.                                  | Data security and application security.....                                    | 62        |
| 2.8.2.                                  | Business benefits and risks of adopting the cloud business intelligence.....   | 62        |

|   |            |
|---|------------|
| 2.8.3. Cloud deployment models.....   | 63         |
| 2.8.4. Cloud service providers.....   | 64         |
| 2.9. Conclusion.....  | 64         |
| <b>CHAPTER 3 RESEARCH METHODOLOGY.....</b>  | <b>66</b>  |
| 3.1. Introduction.....  | 67         |
| 3.2. Research methodology and design.....   | 67         |
| 3.2.1. Research philosophy.....   | 68         |
| 3.2.1.1. Knowledge in information systems research due to pragmatism.....             | 73         |
| 3.2.2. Deductive and inductive research approaches.....                               | 75         |
| 3.2.3. Research design.....   | 76         |
| 3.2.3.1. Mixed-methods research designs.....  | 78         |
| 3.2.3.2. Variants of an exploratory sequential mixed-methods design.....              | 83         |
| 3.2.4. Exploratory sequential mixed-method research strategy.....                     | 83         |
| 3.2.5. Population, sample size and sampling procedures.....                           | 84         |
| 3.2.6. Data generation and analysis methods in exploratory sequential design.....     | 88         |
| 3.2.7.2. Data collection in quantitative phase using survey questionnaire method..... | 97         |
| 3.2.7.3. Quantitative data analysis for the qualitative phase.....                    | 97         |
| 3.2.8. Credibility and trustworthiness in qualitative data.....                       | 97         |
| 3.2.9. Validity and reliability of a questionnaire.....                               | 98         |
| 3.2.10. Ethical consideration.....  | 99         |
| 3.2. Conclusion.....  | 100        |
| <b>CHAPTER 4 DATA ANALYSIS, INTERPRETATION AND FINDINGS.....</b>                      | <b>101</b> |
| 4.1. Introduction.....  | 102        |
| 4.1.1. Findings from the qualitative phase.....                                       | 102        |
| 4.1.2. Demographic information for the study.....                                     | 104        |

|   |     |
|---|-----|
| 4.1.3. SRQ1: What factors influence the adoption and use of cloud business intelligence among small and medium enterprises in small South African towns?..... | 106 |
| 4.1.3.1. Theme 1: Knowledge of benefits of adopting and using Cloud BI.....   | 106 |
| 4.1.3.2. Theme 2: Challenges to the adoption and use of Cloud BI to support business operations.....  | 113 |
| 4.1.4. SRQ2: How do decision-makers evaluate Cloud BI before adoption? .....  | 122 |
| 4.1.4.1. Theme 3: Security evaluation strategies and tools for Cloud BI.....  | 122 |
| 4.1.5. SRQ3: What challenges do decision-makers face when evaluating Cloud BI? .....  | 143 |
| 4.1.5.1. Theme 4: Challenges faced when evaluating cloud business applications ....   | 143 |
| 4.1.6. SRQ4: What do decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises? .....  | 147 |
| 4.1.6.1. Theme 5: Knowledge of tools used to evaluate security in cloud business intelligence.....  | 147 |
| 4.2. Conclusion.....  | 154 |
| CHAPTER 5 DISCUSSION OF FINDINGS.....   | 156 |
| 5.1. Introduction .....   | 157 |
| 5.2. Discussion of findings .....   | 157 |
| 5.2.1. Characteristics of decision-makers and the enterprises.....  | 157 |
| 5.2.2. Factors influencing the adoption and use of Cloud BI among SMEs in small South African towns .....   | 160 |
| 5.2.3. Evaluation of cloud business intelligence by small and medium enterprises before adoption.....   | 161 |
| 5.2.4. Challenges faced by small and medium enterprise decision-makers when evaluating cloud business intelligence .....                                      | 182 |
| 5.2.5. The main components of a security evaluation framework for Cloud BI for small and medium enterprises.....  | 195 |
| 5.3. Conclusion.....  | 200 |

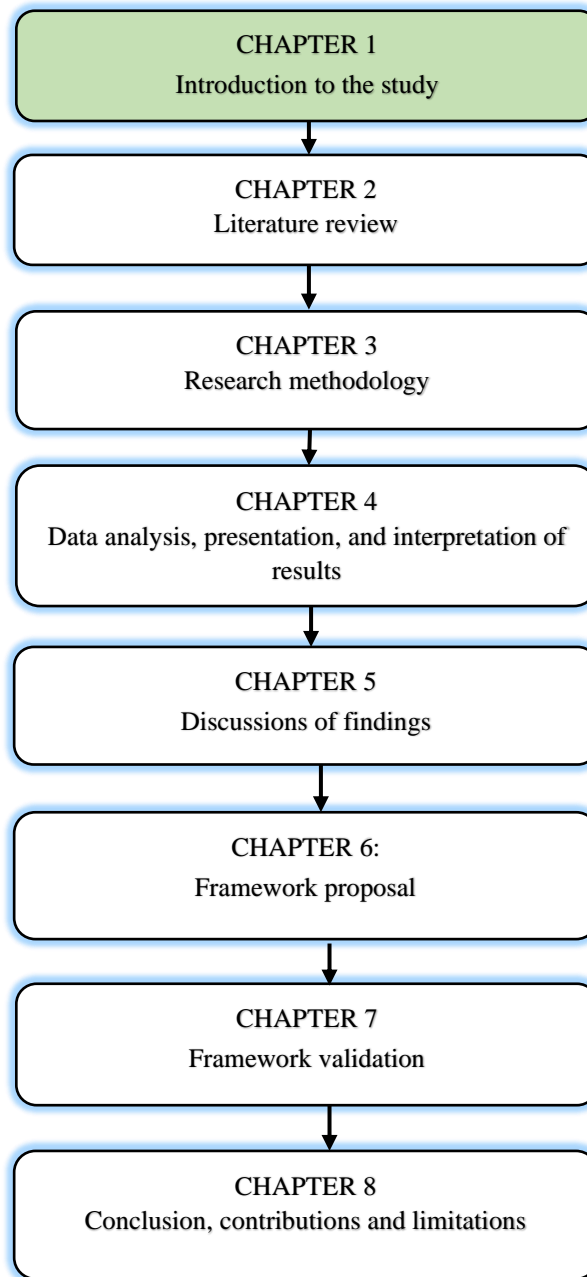


|           |  |     |
|-----------|--|-----|
| CHAPTER 6 | FRAMEWORK PROPOSAL.....  | 202 |
| 6.1.      | Introduction .....   | 203 |
| 6.2.      | Security evaluation framework proposal and analysis.....                   | 203 |
| 6.2.1.    | Factors motivating the proposal and development of the new framework ..... | 203 |
| 6.2.2.    | The Cloud Business Intelligence Security Evaluation Framework.....         | 206 |
| 6.2.3.    | Framework analysis.....  | 207 |
| 6.2.4.    | Using the checklists in the evaluation process .....                       | 229 |
| 6.3.      | Conclusion.....  | 230 |
| CHAPTER 7 | FRAMEWORK VALIDATION .....   | 231 |
| 7.1.      | Introduction .....   | 232 |
| 7.2.      | Framework validation.....  | 232 |
| 7.2.1.    | Content validity as framework relevance validation .....                   | 233 |
| 7.2.2.    | Face validity as framework acceptance validation .....                     | 233 |
| 7.2.3.    | Purpose of validating the security evaluation framework .....              | 234 |
| 7.3.      | Methodology .....  | 234 |
| 7.3.1.    | Validation instruments design and testing.....                             | 234 |
| 7.3.2.    | Population, sample, and sampling procedures for framework validation ..... | 235 |
| 7.3.3.    | Data collection techniques.....  | 236 |
| 7.3.4.    | Data analysis techniques.....  | 236 |
| 7.4.      | Results of framework validation .....                                      | 236 |
| 7.4.1.    | Relevance validity .....   | 236 |
| 7.4.2.    | Acceptance validation using face validity analysis .....                   | 241 |
| 7.4.2.1.  | Suggestions and modifications.....   | 249 |
| 7.5.      | Discussions.....   | 249 |
| 7.6.      | Conclusion.....  | 250 |

|             |  |     |
|-------------|--|-----|
| CHAPTER 8   | CONCLUSIONS, CONTRIBUTIONS AND LIMITATIONS OF THE STUDY .....                                | 252 |
| 8.1.        | Introduction .....   | 253 |
| 8.2.        | Summary of the study.....  | 253 |
| 8.3.        | Conclusions of the study .....   | 254 |
| 8.3.1.      | Factors influencing the adoption and use of Cloud BI among SMEs in the Limpopo Province..... | 254 |
| 8.3.2.      | Strategies used by SME decision-makers to evaluate Cloud BI before adoption ...              | 255 |
| 8.3.3.      | Challenges faced by SME decision-makers when evaluating Cloud BI.....                        | 256 |
| 8.3.4.      | Main considerations made when evaluating Cloud BI.....                                       | 256 |
| 8.3.5.      | The main components of a security evaluation framework for Cloud BI for SMEs.....            | 256 |
| 8.4.        | Contribution to the existing body of knowledge .....   | 257 |
| 8.5.        | Limitations of the study.....  | 258 |
| 8.6.        | Recommendations for future research.....   | 259 |
| REFERENCES  | .....  | 260 |
| APPENDICES  | .....  | 311 |
| Appendix A: | UNISA Ethical clearance.....   | 311 |
| Appendix B: | UNISA amended ethics clearance .....   | 312 |
| Appendix C: | Turnitin Digital Receipt .....   | 315 |
| Appendix D: | Proofreading and editing certificate .....   | 316 |
| Appendix E: | Informed consent form and semi-structured interview schedule .....                           | 317 |
| Appendix F: | Informed Consent and Questionnaire for QUAN phase .....                                      | 320 |
| Appendix G: | Informed Consent and Questionnaires for security framework validation.....                   | 327 |
| Appendix H: | Tables referenced in Chapter 3 .....   | 332 |
| Appendix J: | Tables referenced in Chapter 4 .....   | 333 |

|  |     |
|--|-----|
| Appendix K: Figures referenced in Chapter 6..... | 338 |
| Appendix L: Tables referenced in Chapter 7 ..... | 343 |

# CHAPTER 1 INTRODUCTION TO THE STUDY



## **1.1. Background**

The effects of globalisation and the need to be competitive in a globalised market can influence small and medium enterprises (SMEs) to adopt and utilise technological business solutions to improve decision-making on key business operations (Owusu 2020; Ledwaba & Makgahlela 2017; Boonsiritomachai, McGrath & Burgess 2014). Several studies show that globalisation has skewed business opportunities in favour of large business enterprises (LBEs), with enough financial, technological, and Information Technology (IT) human resources, leaving SMEs to deal with global competition in local and national markets (Mwika, Banda, Chembe & Kunda 2018; Ocloo, Akaba & Worwui-Brown 2014; Green 2009). With the advancement of IT, the world has become a global village, enabling business enterprises in different countries to communicate effectively with each other and with customers in the markets they serve (Mwika et al. 2018; Decker, Haltiwanger, Jarmin & Miranda 2016; Ocloo et al. 2014). However, several South African SMEs have been negatively affected by globalisation (Mabotja 2019; Ledwaba & Makgahlela 2017) and struggle in the digital economy because they are slow to adapt and use new IT solutions that can improve competitive advantage in the global markets (Chan 2017; Decker et al. 2016).

To be competitive in a global and digital economy, SMEs need to use IT solutions to meet market expectations; communicate with other enterprises and customers about important economic activities and products or services needed; and utilise the information sparingly to manage business operations in line with the changing times (UK Essays 2018a; Green 2009). Woods (2016) posits that the competitiveness of an enterprise in a digital economy depends on the speed at which it processes data, uses the information to make decisions on how to meet market demands and how to respond to customers. Furthermore, there are studies showing that SMEs in developing countries are preoccupied with being competitive in global markets and the digital economy but continue using traditional business strategies (Decker et al. 2016; Ocloo et al. 2014). To attain a competitive edge over LBEs, SMEs need to adopt innovative strategies that can be supported by IT solutions to process data and make decisions about products and services that attract customers (Ong, Ismail & Goh 2012; Zembylas & Vrasidas 2005). Chan (2017) believes that SMEs can compete effectively with LBEs in global markets; by using emerging IT applications for connectivity and automation of business processes.

The advent of the Fourth Industrial Revolution means that SMEs need to utilise several emerging technologies to support business processes and activities (Bam & Adao 2019; Mabotja 2019; Berdykulova, Sailov, Kaliashdarova & Berdykulov 2014). South African SMEs constantly face IT-related challenges similar to those reported in other developing countries (Small Enterprise Development Agency 2020; Salum, Zaidi & Rozan 2016; Ibrahim & Musah 2015). According to Ocloo et al. (2014), SMEs in developing countries tend to be unfamiliar with the benefits of new IT systems. Decker et al. (2016) regard emerging ITs as one of the challenges that SMEs experience and must deal with to improve competitiveness in local and international markets. Literature shows that traditional IT solutions are difficult for SMEs to use as they demand technical know-how and skill in addition to high costs of acquisition (Small Enterprise Development Agency 2020). Cloud computing technologies have revolutionised the IT industry; by providing user-friendly services while reducing the cost of IT infrastructure overheads (Werff et al. 2019; Dudharejia 2018; Hussein & Khalid 2016).

Cloud computing, or simply the "Cloud", is a computing technology that uses the Internet and remote servers to maintain data and applications (Patil & Chavan 2020; Kumar & Padmapriya 2014). The Cloud allows business enterprises, government organisations, and individual customers to use infrastructure, platforms, and software as services to store and process large volumes of data using a variety of devices that connect to the Internet and the web (Patil & Chavan 2020; Pantić & Babar 2019; Gartner 2016; Kumar & Padmapriya 2014). Software-as-a-Service (SaaS) applications on offer today, include Cloud Business Intelligence, known as Cloud BI (Columbus 2018; Kasem & Hassanein 2014); Customer Relations Management (CRM); Enterprise Resource Planning (ERP); and online data backup. These cloud services provide SMEs with viable alternative solutions to choose from, particularly in poorly resourced South African towns (Mohlameane & Ruxwana 2014, 2020; Lechesa, Seymour & Schuler 2012). There is a high expectation that these cloud computing technologies can transform enterprise information systems to improve data management and decision-making at lower costs than traditional information systems (Tutunea & Rus 2014; Walczak 2014; Scholz, Scieder, Kurze, Gluchowski & Boehringer 2010). Although this is tempting for SMEs to adopt and use cloud computing technologies, it may take time for the benefits to realise because of other factors affecting business success that need to be considered (Berkowsky, Sharit & Czaja 2017; Devesh, Samalia & Verma 2017).

Literature reports an increase in cloud computing awareness and positive acceptance of a range of cloud services among South African SMEs (Mohlameane & Ruxwana 2014, 2020; Turner 2018; Dawson & Van Belle 2013). A report by the Small-Enterprise-Development-Agency (2018), based on a survey of 1157 SME owners and managers in South Africa, showed that 86% used smartphones to support their business operations most of the time; 20% used e-commerce regularly; and 22% made regular use of cloud services, including online storage, ERP, CRM and Cloud BI. The report confirmed that SMEs seek to be more competitive in knowledge and digital economies by utilising Cloud BI to gain a market share predominantly controlled by LBEs. Other studies caution that South African SMEs can expose sensitive data and applications to cybersecurity threats when migrating to the cloud, which can negatively affect essential business transactions and operations (Mirai Security 2019; Afolaranmi, Ferrer & Martinez-Lastra 2018; Vatuiu, Udrica & Tarca 2013). This confirms that there are underlying factors that hinder the uptake and utilisation of Cloud BI by SMEs in small South African towns.

Studies in cloud computing services suggest models and frameworks of adoption that are suitable for LBEs with vast IT infrastructures and managed by IT specialists and security specialists (Chang, Kuob & Ramachandran 2015; Choi & Lee 2015; Winkler 2011) but are silent on how potential adopters, such as SMEs, can evaluate Cloud BI. Nevertheless, some studies encourage decision-makers to conduct a basic security evaluation of Cloud BI in terms of functionality, usability, business value, and security using any tools and methodologies available and affordable to them (Llave 2019; Senarathna, Yeoh, Warren & Salzman 2016; Olszak & Ziemia 2012).

Currently, there are few research studies specifically based on the evaluation of Cloud BI for South African SMEs, despite the emphasis on the adoption of this technology. However, there are several studies on the traditional security evaluation strategies such as vulnerability assessment and penetration tests (VAPT), which are appropriate for LBEs with strong financial resources and IT security specialists (Calumpang & Dilan 2016; Kazim & Zhu 2015). VAPT is an operational-use-evaluation (OUE) technique suitable for enterprises that have adopted IT applications (Mussa, Kipanyula, Angello & Sanga 2016; Rafique, Humayun, Gul, Abbas & Javed 2015). Therefore, VAPT techniques may not be appropriate for SMEs considering the adoption of Cloud BI (Rostek,

Wiśniewski & Kucharska 2012). For a cloud service security evaluation to be effective, Heiser (2019) suggests that the process should be pragmatic, flexible and should utilise multiple forms of security information about Cloud service providers (CSPs). SMEs need to conduct a prior-operational-use evaluation (POUE) or strategic evaluation to determine whether the Cloud BI matches the business niche (Wise 2016; Al-Yaseen 2012; Al-Yaseen, Al-Jaghoub, Al-Shorbaji & Salim 2010).

The presence of many adoption models of cloud computing, which do not elaborate on how decision-makers could evaluate Cloud BI, may contribute to the challenges faced by SMEs. A report by Lamb (2016) emphasises the need to conduct a research study to explore the enablers and barriers to cloud technology adoption from the perspectives of SME owners, managers and employees. This assertion shows how important it is for researchers to understand how SMEs in poorly-resourced small towns adapt to new technologies and the challenges they face so that interventions can be put in place. By following the suggestion by Lamb (2016), it is possible to fill the existing knowledge gap in the security evaluation of Cloud BI by decision-makers in SMEs in South Africa, which has remained an unexplored research area for some time. South African SMEs face unique challenges in the evaluation of Cloud BI, and this requires home-grown solutions involving the affected enterprises. This makes it a worthwhile endeavour to seek a practical solution to the existing problem by proposing an easy-to-use security evaluation framework that can be used by SME decision-makers to evaluate Cloud BI before adoption and use.

## **1.2. The problem statement**

In South Africa, SMEs play an important economic role and are expected to improve their operations by using online IT solutions such as ERPs, Cloud BI, and CRMs. These SMEs are managed by owners and managers who are not IT specialists and are responsible for making important decisions regarding which technology to adopt and how to use it (Mohlameane & Ruxwana 2020; Salim, Sedera, Sawang, Alarifi & Atapattu 2015; Dawson & Van Belle 2013). The presence of several Cloud BI solutions on the web presents SME decision-makers with selection challenges (Moore 2014; Agostino, Soilen & Gerritsen 2013), mostly because they have limited IT technical know-how and skill to evaluate the technologies by themselves. The challenge is compounded by the lack of IT security specialists in SMEs who can assist decision-makers in



selecting appropriate Cloud BI suitable for their business purposes (Sherman 2015; Ghaffari, Delgosha & Abdolvand 2014). This means that when adopting Cloud BI, SME decision-makers who lack IT technical expertise have to actively take part in the evaluation process, which is a big challenge considering the complex nature of cloud computing technology and services. Unlike traditional business intelligence (BI) applications, which requires enterprises to evaluate mainly technical and procedural aspects, Cloud BI involves the evaluation of more areas, including security vulnerabilities, threats, and risks (Vacca 2017; Ibrahim & Musah 2015).

Most industry security frameworks and standards in use today are suitable for big and complex IT systems and can be difficult for SME decision-makers to evaluate Cloud BI since IT security specialists would be required for the implementation (Elmalah & Nasr 2019; Mirai Security 2019; Rizvi, Ryoo, Kissell, Aiken & Liu 2018; Olszak 2014). In SMEs, critical decisions have to be made regarding which Cloud BI to adopt and which not to use, and this places the decision-makers at the centre of the security evaluation process (Venturebum 2015; Malik & Nazir 2012). SME decision-makers are unable to use existing traditional or industry security frameworks and standards since these are complex and probably inappropriate for South African SMEs. Without proper knowledge and skills to use industry evaluation tools, decision-makers can find it challenging to evaluate and select appropriate Cloud BI. Faced with such predicaments, decision-makers are likely to recommend SMEs to adopt and use Cloud BI without sufficient knowledge of inherent security vulnerabilities or leave SMEs technologically marginalised by not adopting and using cloud technologies.

This study is, therefore, necessary to address the problem created because of the lack of user-friendly security evaluation frameworks for Cloud BI for use by SMEs in small South African towns, where there is a scarcity of IT security specialists available to these enterprises when they plan to adopt and use such technology. The proposed security evaluation framework provides SMEs with an alternative tool to overcome challenges that they face in the selection of Cloud BI as it will indicate the aspects to be evaluated using simple checklists.

### **1.3. Purpose of the study**

The purpose of this study was to propose a security evaluation framework for Cloud BI that can be used by SMEs in small, under-resourced South African towns.

#### **1.4. Research objectives and research questions**

The major research objective of the study was:

*To propose a security evaluation framework for Cloud BI suitable for use by SMEs in small under-resourced South African towns.*

Four sub-research objectives were:

- a. To explore factors influencing the adoption and use of Cloud BI by SMEs in small South African towns;
- b. To examine the strategies used by SME decision-makers in evaluating Cloud BI they have adopted or intend to adopt;
- c. To evaluate the critical security evaluation challenges that prevent the adoption of Cloud BI by these SMEs; and
- d. To determine the main components of the security evaluation framework of a Cloud BI so for use by decision-makers who are not IT specialists.

The study was guided by the major research question stated as:

*What are the main components of a security evaluation framework for Cloud BI suitable for small and medium enterprises in under-resourced South African towns?*

To answer this research question, four sub-research questions (SRQs) were formulated as stated:

**SRQ1:** *What factors influence the adoption and use of Cloud BI among SMEs in small South African towns?*

The purpose of this SRQ was to explore the critical factors that influence the adoption and utilisation of Cloud BI among SMEs, in general, and particularly in small South African towns where owners and managers have limited knowledge about security in cloud services. Related literature provided the benefits and risks of Cloud BI and other cloud services for SMEs. Empirical findings provide insights about the level of adoption of Cloud BI and other cloud services for SMEs in small South African towns, particularly in the Limpopo Province in which the study was conducted. Chapter 2 deals with related literature, while the findings from the empirical study are presented in Chapter 4 and discussed in Chapter 5.

**SRQ2:** *How do small and medium enterprise decision-makers evaluate Cloud BI before adoption?*

SRQ2 required the researcher to critically examine existing security evaluation tools and strategies available to SMEs and their limitations. The strategies currently used by SMEs in evaluating Cloud BI are important in providing background about current practices essential to inform the proposed security evaluation framework. As the proliferation of various low-cost and self-service Cloud BI increases, so does the awareness and interest among SMEs for the business benefits of these applications in decision-making. For SMEs to select the most appropriate Cloud BI, respective decision-makers have to evaluate these applications based on certain criteria that this study examined. Literature for SRQ2 is presented in Chapter 2 while the results are presented and discussed in Chapters 4 and 5 respectively.

**SRQ3:** *What challenges do small and medium enterprise decision-makers face when evaluating Cloud BI?*

To answer SRQ3, a literature review was conducted to identify critical factors that influence the adoption of Cloud BI by SME decision-makers, both globally and in the South African context. An in-depth analysis of theoretical foundations was provided by comparing various technology adoption models and frameworks such as Theory of Planned Behaviour (TPB), Diffusion of Innovation Theory (DoIT), Technology Acceptance Model (TAM) and Multi-Stage Adoption Model (MSAM). The other SRQs, the empirical results and findings for SRQ3 are presented and discussed in Chapters 4 and 5 respectively.

**SRQ4:** *What do decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises?*

Lamb (2016) encourages researchers to extract important information about the social phenomena being studied directly from those who use the technology to develop or verify a theory. By answering SRQ4, the study provides insights into what decision-makers consider important when evaluating and selecting Cloud BI and services. The empirical findings were used to propose a security evaluation framework.

### **1.5. Research focus**

The focus of this thesis was to propose a security evaluation framework that SMEs could use to evaluate Cloud BI. To achieve this, an empirical study was conducted with SME decision-makers from five selected towns in the Limpopo Province. The findings of this study were used to identify the components of the security evaluation framework for Cloud BI.

### **1.6. Scope and context of the study**

This study explored the factors influencing the adoption of Cloud BI by SMEs in the Limpopo Province, SME decision-makers' knowledge of security evaluation of Cloud BI and evaluation strategies used, and the challenges faced during the adoption process. The study was conducted with SME decision-makers from five selected towns in the Limpopo Province who used IT solutions to aid business operations. The study was conducted between January 2016 and March 2021.

### **1.7. Research methodology**

This study adopted the pragmatic paradigm and a mixed-methods research methodology in which an exploratory sequential design was used to plan data collection and analysis. The exploratory sequential design consisted of two phases, namely a qualitative (QUAL) and a quantitative (QUAN) phase, each designed to collect different types of data (Creswell 2013; Creswell & Plano-Clark 2011; Teddlie & Tashakkori 2009). A detailed discussion of the research methodology and ethical considerations is presented in Chapter 3 of this study.

### **1.7.1. Population, sample size and sampling procedures**

The population selected for this study consisted of SME decision-makers from five towns in the Limpopo Province, namely Louis Trichardt, Mokopane, Musina, Giyani and Thohoyandou, who were using IT solutions to support their business operations. The study used two samples, namely a purposive sample of thirteen (13) SME decision-makers from which qualitative data for the QUAL phase was collected using a semi-structured interview; and a convenience sample of fifty-seven (57) owners and managers using a questionnaire to collect quantitative data for the QUAN phase. A detailed discussion of the population and sampling procedures is provided in Chapter 3.

### **1.7.2. Data generation and analysis techniques**

Qualitative data were collected using semi-structured interviews and analysed thematically using the Atlas.ti 8 package. A survey questionnaire was used to collect quantitative data, and results were analysed quantitatively, using SPSS Version 26 and presented as frequency tables, descriptive statistics, and inferential statistics. Detailed discussions of data generation and analysis are provided in Chapter 3.

## **1.8. Contribution of the study**

Existing studies encourage SMEs to adopt and use Cloud BI and other cloud services. However, they do not provide simple evaluation frameworks to do so. Therefore, this research study proposed a security evaluation framework for evaluating Cloud BI for use by SMEs where there are no IT specialists available. The major outcome of the study was a framework to assist SMEs to evaluate the security of Cloud BI they intend to adopt and use. This study has both scientific and business value.

### **1.8.1. Scientific value**

While attempting to solve an existing real-life and practical problem faced by SMEs in Cloud BI in the adoption and use, this study sought to extend scientific knowledge about security evaluation frameworks for Cloud BI. The scientific contribution entails systematic analysis, interpretation, evaluation, and synthesis of existing literature on security frameworks in Cloud BI and other related IS applications focusing on SMEs. Based on existing knowledge and empirical evidence from SMEs, the findings of this study should contribute towards the generation of new literature and knowledge that could positively impact the evaluation of Cloud BI by SMEs in the Limpopo

Province. The security evaluation framework is a major contribution to scientific knowledge in Information Systems research. This study:

- contributed to the body of knowledge on Cloud BI by providing systematic methods and mechanisms for evaluating security in these applications in the context of SMEs in the Limpopo Province.
- expanded the existing body of literature on security evaluation of Cloud BI in the context of non-IT specialist end-users who manage SMEs, and the understanding of the implementation of security mechanisms to assess and evaluate security threats in Cloud BI by SMEs; and
- provided developers with alternative and simple design guidelines for security evaluation frameworks for Cloud BI for use by systems end-users without IT security knowledge.

### **1.8.2. Business value**

The business value is derived from the fact that the proposed framework is likely to highlight and provide alternative ways of viewing security in Cloud BI by SME decision-makers. The security evaluation framework could encourage SMEs to adopt and use Cloud BI, which in the long run should enable them to participate successfully in e-commerce. The use of the proposed security evaluation framework to evaluate security threats and financial risks could provide SMEs with a strong basis to make informed decisions on whether to adopt Cloud BI.

### **1.8.3. Academic community**

The outcome of this research study was intended to contribute to the knowledge of security evaluation frameworks and should raise new ways of thinking about SMEs' participation in Cloud BI evaluation. The academic community would be provided with a platform to base new research on; information security about Cloud BI security evaluation. The study provides new literature on the adoption of Cloud BI by disadvantaged communities in South Africa, which can lead to further research in this area.

## 1.9. Benefits of the study

This study was intended to benefit stakeholders concerned with cloud services, namely:

- Developers of security evaluation tools, who will be able to integrate the requirements and criteria identified by this research as design guidelines when developing new business solutions; and
- SMEs intending to adopt Cloud BI, to use the framework to evaluate security threats and risks in technologies before adopting and using the applications.

## 1.10. Definition of the terminology used in the thesis

This study used terms that could have different meanings to those with which readers are familiar. This subsection provides a list of definitions of key terms used in this research study.

**Business Intelligence** is “the capability of an enterprise to use its human resources together with a broad category of processes, applications and technologies for accessing, collecting, accumulating and analysing data to generate actionable and competitive information that can support its users to make better decisions” (Balachandran & Prasad 2017; Boonsiritomachai et al. 2014).

**Cloud business intelligence** is the merging of cloud computing architectures and business intelligence technology flexibly and cost-effectively to support fast and efficient decision-making in organisations (Patil & Chavan 2020).

**Evaluation** is a methodical process based on empirical evidence to provide credible, reliable, and useful information that facilitates the decision-making process in organisations (Alkin & King 2017).

A **security evaluation framework** is a succession of clear processes that describe policies and procedures needed in the implementation and continuation of the management of information security measures in an information system used in an organisation (Khan 2012).

**An SME** is an independent business enterprise managed by one owner, appointed individual and can have its branches, conduct business activities in any sector or subsector of the economy in South Africa (South African Government Gazette No.42304 Department of Small Business Development 2019; Ajumobi & Kyobe 2017).

**SME decision-makers** refer to owners and family-appointed individuals who manage the daily operations of small and medium enterprises and make decisions on the types of IT to adopt and how they will be used (Hauser, Eggers & Guldenberg 2020).

**Vulnerability** is a combination of the attractiveness of a facility as a target and the level of deterrence and (or) defence provided by the existing security controls (Renfroe & Smith 2016).

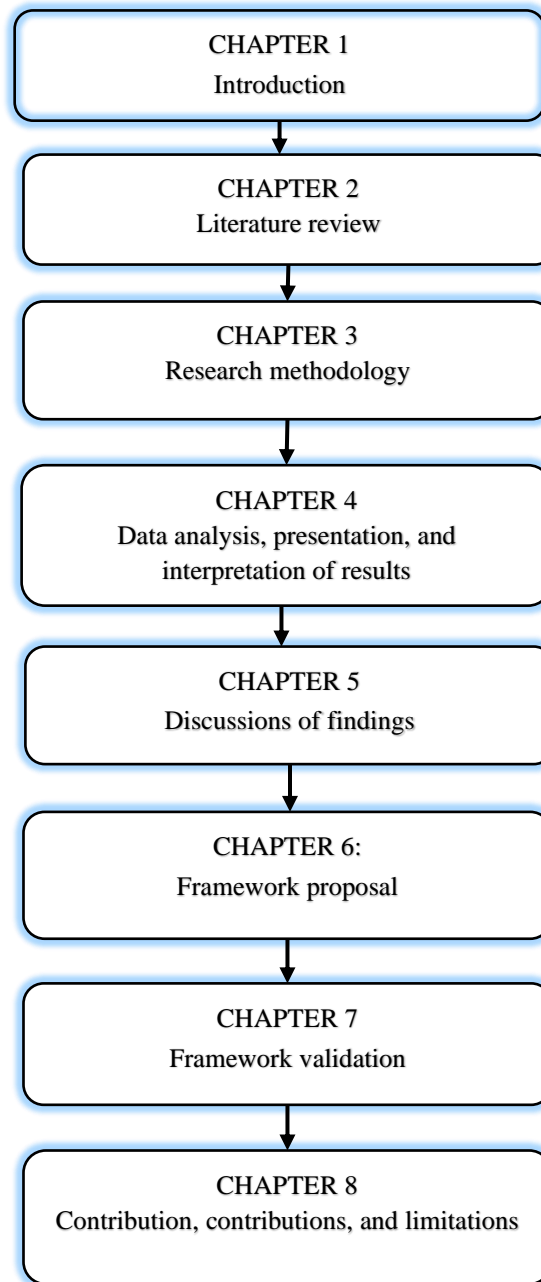
**Technology adoption** refers to a sequence of stages through which an innovation or new technology passes before the new product, service or idea will be accepted by a potential adopter before being used (Straub 2017; Frambach & Schillewaert 2002)

### **1.11. The layout of the thesis**

This thesis will consist of eight chapters (see Fig 1.1). Chapter 1 introduces the study and provides the background to the problem, the problem, the purpose of the study, the research questions, and the contribution to the existing field of knowledge. Chapter 2 deals with the literature regarding Cloud BI, its potential contribution to modern IS and the dangers they pose to organisations in terms of information security and financial risks. The chapter further explores cloud deployment and service models as well as concepts related to Cloud BI, such as access controls, deployment models, service delivery, portability, interoperability, vendor, and data lock-in, reliability of confidentiality, availability, integrity, dashboards, security threats and risks.

Chapter 3 focuses on Research Methodology which describes the methodology used to conduct the empirical study, collect data, design, and create the security framework. It further describes data collection methods, construction of the research instruments, tests for validity and reliability of the instruments, trustworthiness, credibility, and ethical issues. Chapter 4 deals with the empirical study of data analysis, presentation of results and interpretations. Chapter 5 presents detailed discussions of the findings made in the study. Chapter 6 proposes and analyses the security evaluation framework. The validation of the framework is presented in Chapter 7. The contributions, conclusions and limitations of the research study are dealt with in Chapter 8.





**Figure 1.1: Thesis layout structure**

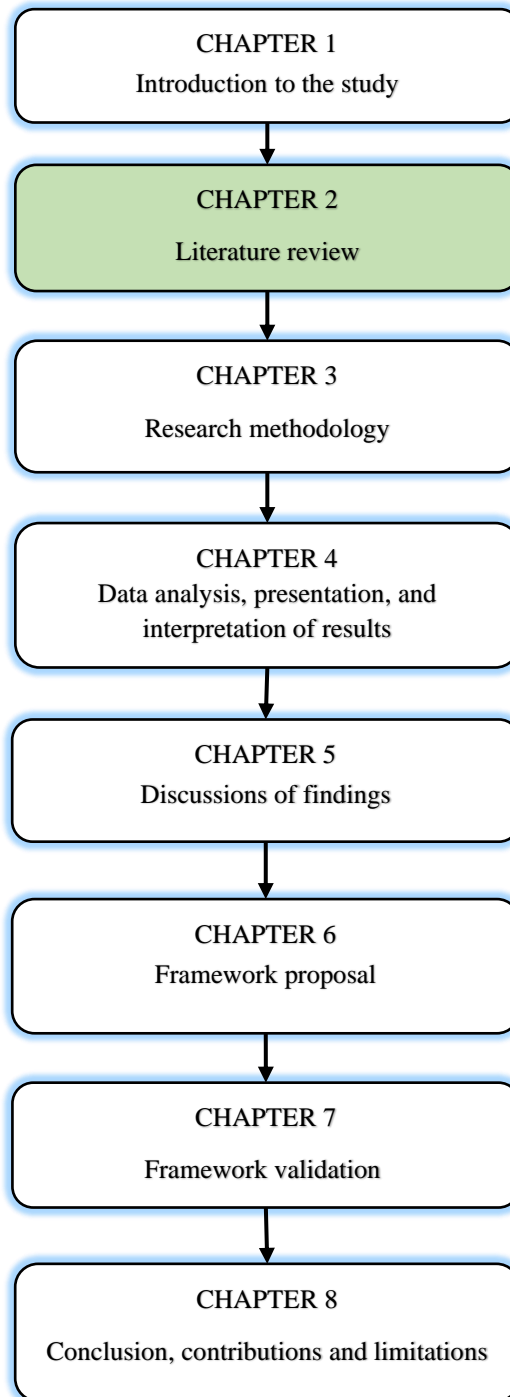
### **1.12. Summary**

Currently, low-cost Cloud BI are available for use by SMEs of varying sizes and types to support decision-making to improve key business operations and activities. Unlike in LBEs, where there are IT-security specialists, SMEs tend to lag in adopting and using IT solutions. Many factors influence SMEs when deciding to adopt business solutions. To ameliorate this problem, a

framework to evaluate Cloud BI was proposed based on the findings of the study. SMEs require a framework that is simple, devoid of technical jargon, easy-to-use, robust and cheap. Therefore, the purpose of the study was to develop a security evaluation framework for Cloud BI applications that SMEs could use.

This chapter outlined the background to the problem and justified the need to conduct this research study. The problem was identified and explained to illustrate the importance of Cloud BI and justify the adoption of these technologies by SMEs. The exploratory mixed-method research design was used as it allowed the study to be conducted flexibly with both qualitative and quantitative designs sequentially. The main contribution to knowledge by this study is the proposal of a security framework that can be used by SMEs. This study was conducted with SME decision-makers in the Limpopo Province. The literature review of this study is presented in Chapter 2.

## CHAPTER 2 LITERATURE REVIEW



## **2.1. Introduction**

In Chapter 1, the background of the study was outlined, and the main research question was posed: *What are the main components of a security evaluation framework for Cloud BI suitable for small and medium enterprises in small South African towns?*

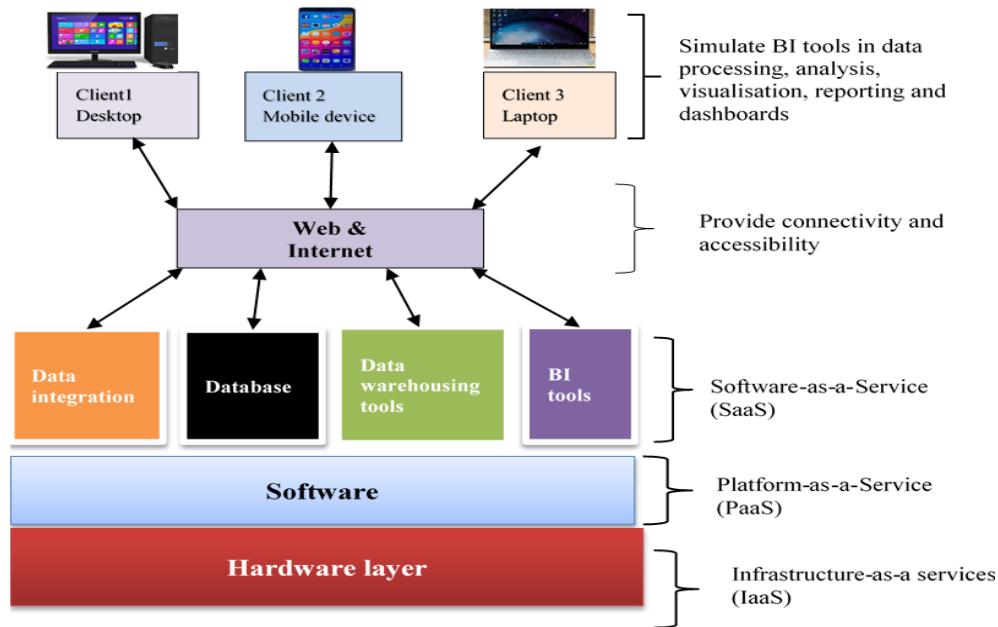
In this chapter, the literature related to the research will be reviewed in terms of the key concepts as well as the four sub-research questions posed in Chapter 1. The literature presented in this chapter deals with factors influencing the adoption of Cloud BI by SMEs, the strategies used in evaluating Cloud BI, and the challenges they pose. Theories and models of technology adoption are used to provide insights into the technology adoption process and the underlying issues involved. The gap relating to the security evaluation of Cloud BI was identified within the existing literature.

## **2.2. Definition of cloud business intelligence**

Various terms, such as Business intelligence in the Cloud (Llave 2019; Thompson & van der Walt 2010), Software-as-a-Service Business Intelligence (SaaS BI) (Kasem & Hassanein 2014), Business intelligence on the Cloud (Tamer, Kiley, Ashrafi & Kuilboer 2013), and Business intelligence over the cloud (Hooda 2014) are used to denote Cloud BI (Patil & Chavan 2020; Gurjar & Rathore 2013). Cloud BI is the most commonly used term when referring to business intelligence offered over cloud computing technology (Patil & Chavan 2020; Columbus 2018; Phocas Software 2015). Overlaps in the definitions of Cloud BI exist, despite the use of these different terms. For example, Rouse (2011) refers to Cloud BI as SaaS BI, a delivery model in which Business intelligence is deployed outside an enterprise's firewall hosted at a location and accessed by clients over an Internet connection. Similarly, Walczak (2014) regards a Cloud BI as the delivery of business intelligence capabilities in SaaS, one of the cloud computing service delivery models. The purpose of a Cloud BI is to provide business intelligence features as a service, utilising cloud computing technology at low cost with rapid deployment and more flexibility compared to traditional business intelligence (traditional BI) applications (Gurjar & Rathore 2013). It can be deduced that a Cloud BI is an IT solution with improved capabilities, cheaper and more user-friendly than the traditional BI applications and other conventional information systems (Javaid 2014; Menon, Rehani & Gund 2012). Most importantly, Cloud BI is among the newest technological evolutions of business intelligence technologies used to access and process raw data

into useful information needed when making important business decisions (Patil & Chavan 2020; Al-Aqrabi, Liu, Hill & Antonopoulos 2015). A combination of the definitions proposed by Gurjar and Rathore (2013) and Walczak (2014) indicates the mode of delivery and the benefits derived from Cloud BI.

Literature categorises Cloud services as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) (Werff et al. 2019; Kasem & Hassanein 2014). This shows that Cloud BI as a service depends on each of the three cloud computing technologies but may assume different versions of the architecture. A simplified Cloud BI architecture presented in Figure 2.1 illustrates important components.



**Figure 2.1: Generalised Cloud BI Architecture**

Adapted from Kumar and Padmapriya (2014) and Kasem and Hassanein (2014) for this study

The Cloud BI architecture in Figure 2.1 depicts basic hardware and software components that CSPs provide as services and how the clients can access the applications in the cloud (Kasem & Hassanein 2014; Gurjar & Rathore 2013). The essential components of Cloud BI architecture are:

- i. *IaaS* the basis of cloud services, consists of the basic hardware which provides high processing power, large scalable physical data storage, system management, legacy, virtual machines, servers and reliable network connections (Kumar & Padmapriya 2014; Labes, Repschläger, Zarnekow, Stanik & Kao 2012). *IaaS* is regarded as suitable for large enterprises, which needs hardware with large processing power and big storage space (Ahmed & Hossain 2014; Kumar & Padmapriya 2014).
- ii. *PaaS* is an important software layer, which includes operating systems and drivers needed to run hardware and end-user applications such as Cloud BI, Databases, data warehouses, web servers and execution runtime. Besides, the *PaaS* provides a platform for development tools needed to develop applications that are provided as services. *PaaS* can be used to develop or customise applications for enterprises (Wanjiku & Moturi 2016; Kumar & Padmapriya 2014).
- iii. *SaaS* is a cloud service offered as software over the Internet and the web to enterprises and individuals who want to outsource applications to reduce costs of installation and purchasing software (Pantić & Babar 2019; Wanjiku & Moturi 2016; Gartner 2016). *SaaS* applications are touted as being the most suitable for SMEs with limited resources to acquire on-premise IT infrastructure (Widyastuti & Irwansyah 2018; Choi & Lee 2015). The business solutions such as CRM, ERP and BI are offered in *SaaS* as services that can be used to manage enterprise data and other purposes. This study deals with *SaaS* BI or Cloud BI adoption by SMEs in small South African towns. The Cloud BI requires:
  - Data integration to perform extract, transform, load and data cleansing procedures in the Cloud (Bucur 2012; Menon et al. 2012);
  - Database systems are used to store enterprise data in the cloud (Elmalah & Nasr 2019);
  - Data warehousing tools in the form of applications for creating and maintaining the data warehouse (Rostek et al. 2012); and
  - BI tools are used to set up front-end applications for reading and analysing data kept in the data warehouse (Kasem & Hassanein 2014; Pant 2009).

There is a strong belief that Cloud BI can provide SMEs with an alternative business solution to traditional BI (Patil & Chavan 2020; Tutunea & Rus 2014; Olszak & Ziembra 2007). According to

Grabova, Darmont, Chauchat and Zolota, (2010), SMEs need cheap, lightweight architectures and tools providing online data analysis for easy and quick decision-making. Cloud BI has such characteristics which make them ideal for use by SMEs in any type of industry in South Africa, but each enterprise needs to evaluate and select the most appropriate one for its business needs.

### **2.3. Cloud deployment models**

When selecting a Cloud BI, an enterprise has to choose a cloud deployment model in which the services, data and application will be provisioned (Sweetman 2019; Devesh et al. 2017; Rostek et al. 2012). By examining this key concept, the benefits and underlying security issues that SMEs should consider when adopting Cloud BI will be illustrated in subsequent subsections of the thesis.

Cloud BI can be deployed over any of the three cloud deployment models, namely private, community, public or hybrid (Papachristodoulou, Koutsaki & Kirkos 2017; Carcary, Doherty & Conway 2014; Kasem & Hassanein 2014) and this is reported to have security bearings on the enterprise data and information which SMEs have to deal with (Yauri & Abah 2016; Mohlameane & Ruxwana 2014; Alshamaila, Papagiannidis & Li 2013).

- i. *Private clouds* are either leased or owned by an enterprise and have the lowest extent of allotment but are reported as being expensive for SMEs to utilise (Romes 2015; Shahbazi, Brinkley & Tabrizi 2013). Although private clouds provide the most secure cloud environment, most of the SMEs in small towns may not be able to afford this technology due to budget constraints (Iqbal et al. 2016; Kasem & Hassanein 2014; Mohlameane & Ruxwana 2013).
- ii. *Community* clouds bring together organisations and allow them to share the same technology with mutual trust (Ibrahim & Musah 2015; Romes 2015). These clouds are less accessible by SMEs because of the cost involved.
- iii. *Public clouds* allow the deployment of the Cloud BI so that it is accessible to the public, and this makes them the most extensively shared and relatively cheap, but most unsecure technology (Bach, Celjo & Zoroja 2016; Vasista 2015; Li, Liang, Yang & Chen 2010). The public cloud is the most commonly used deployment due to its maturity (Pantić & Babar 2019). Although not conclusive, an online survey by Columbus (2017) reports that the public

cloud is the most preferred deployment model for Cloud BI by SMEs, where data security breaches are prevalent.

- iv. A *hybrid cloud* is built from two or more cloud infrastructures that remain discrete entities but are connected by standardised or proprietary technology to enable data and application portability to some extent (Clohessy 2017; Gartner 2016; Romes 2015). Still, the costs of hybrid clouds could be more than what SMEs might be able to invest, and the security features are unknown to SMEs (Antoo, Cadessaib & Gobin 2015; Li et al. 2010).

The attributes of the four cloud deployment models and traditional information systems (IS) are shown in Table 2.1.

**Table 2.1: Attributes of cloud deployment models and traditional information systems**

| ATTRIBUTES                     | CLOUD DEPLOYMENT MODELS |                    |        |                |
|--------------------------------|-------------------------|--------------------|--------|----------------|
|                                | Private                 | Community / Hybrid | Public | Traditional IS |
| Initial costs                  | High                    | Medium             | Low    | High           |
| Ongoing costs                  | Low                     | Medium             | Low    | High           |
| Security                       | High                    | Medium             | Low    | High           |
| Compliance                     | High                    | Medium             | Low    | High           |
| Quality of Service             | High                    | Medium             | Low    | High           |
| Integration                    | High                    | Medium             | Low    | High           |
| Configurability                | Medium                  | Medium             | Low    | High           |
| Data control                   | High                    | Medium             | Low    | High           |
| Security assurance by users    | Low                     | Medium             | High   | None           |
| Security assurance by CSPs     | High                    | Medium             | Low    | None           |
| Data mining issues by CSPs     | Low                     | Medium             | High   | None           |
| Mixing of clients' data        | Low                     | Medium             | High   | None           |
| Vendor-lock-in                 | Low                     | Medium             | High   | None           |
| Interoperability issues        | Low                     | High               | High   | None           |
| Data portability issues        | Medium                  | High               | High   | Low            |
| Application portability issues | Medium                  | High               | High   | Low            |
| Hardware sharing issues        | Low                     | Medium             | High   | None           |
| Software sharing issues        | Low                     | Medium             | High   | None           |
| CSP security breaches issues   | Low                     | Medium             | High   | Low            |
| Hacker security breach issues  | Low                     | Medium             | High   | None           |
| Exposure to security threats   | Low                     | Medium             | High   | Low            |

**Adapted from Oracle White Paper (2010)**



Table 2.1 shows that private clouds have the disadvantage of the high initial cost for acquiring infrastructure and software that SMEs may be unable to pay, while public clouds are cheaper and more affordable. However, security issues in the public cloud always outweigh the cost benefits of the acquisition and running of the Cloud BI in this model. Although the Cloud BI opportunities for SMEs seem to be favourable in public and community deployments, enterprises have to decide on the information assets that should be migrated to the cloud as well as how to deal with security challenges.

#### **2.4. State of adoption of cloud business intelligence**

Literature specific to the adoption and use of Cloud BI by South African SMEs is scarce compared to that of on-premises and cloud computing in general (Pirttimaki 2010; Thompson & van der Walt 2010). The few literature sources available reveal that even on-premise BI applications have remained unpopular among South African SMEs; as evidenced by poor adoption and use (Salum et al. 2016; Carcary et al. 2014). However, the Small-Enterprise-Development-Agency (2018) reports that the acceptance of various cloud services by SMEs in South Africa is expected to rise, particularly those that require simple skills but will not translate to meaningful adoption and use.

#### **2.5. Factors influencing the adoption of Cloud business intelligence**

The adoption of Cloud BI by SMEs is influenced by an array of factors, some beneficial and others detrimental (Heang 2017; Sheshasaayee & Swetha 2015). Consequently, SME decision-makers need to have adequate knowledge about how Cloud BI works, its long-term benefits and various security issues inherent before adopting and using this technology. Theories of technology adoption are critically examined to understand factors that might promote and prevent the adoption and use of Cloud BI by SMEs.

##### **2.5.1. The technology adoption theories**

Technology adoption theories conceptualise and explain the process of technology adoption differently but acknowledge that an individual or enterprise must evaluate the benefits and risks of the technology, before deciding on its adoption (Momani & Jamous 2017; Romes 2015; Salim et al. 2015). Several theories and studies indicate the complexity of the process of technology adoption and the challenges it can present to SMEs when adopting Cloud BI (Venkatesh, Morris,

Davis & Davis 2018; Lai 2017; Williams & French 2014). Ettlie (1980) presents the technology adoption process with five stages, including awareness, interest, evaluation, trial and commitment (Salim, Sedera, Sawang & Alarifi 2014; Sahin 2006; Ettlie & Penner-Hahn 1994; Ettlie 1980). According to Rogers (1995), technology adoption is a process by which an innovation is communicated using existing methods within a given community over time (Fry, Ryley & Thring 2018; Lai 2017; Salim et al. 2015). Similarly, Fichman and Kemerer (2012) posit that technology adoption is a collection of activities undertaken during the adoption process, which starts with awareness of the existence of the technology and leads to the successful deployment of the technology within the enterprise.

Research in Information Systems (IS) has been preoccupied with establishing how and why individuals or enterprises choose to adopt and use emerging technologies (Fry et al. 2018; Taherdoost 2018; Olushola & Abiola 2017). At the core of the technology adoption theories are beliefs, perceptions and knowledge about the benefits and risks that innovations or new technologies could bring to the enterprise (Ren 2019; Momani & Jamous 2017). Studies applying these theories report several factors that influence enterprises and individuals when deciding to adopt new technologies (Patil & Chavan 2020; Nyoro, Kamau, Wanyembi, Titus & Dinda 2015; Salim et al. 2014; Oliveira & Martins 2011). Most of these theories originated from developed countries where they have been useful in predicting IT adoption by SMEs in those countries, but have not been thoroughly tested in developing countries that have different business settings and technological expectations (Hamida, Razakb, Bakar, Salihin & Abdullah 2016; Carcary et al. 2014). Despite the importance placed on the adoption process in several studies, the contribution made to the adoption of Cloud BI among SMEs in small South African towns remains a conjecture.

#### **i. Theory of Planned Behaviour**

Theory of Planned Behaviour (TPB) is one of the most influential technology adoption theories used to predict behavioural intentions and behaviours of individuals in the uptake of any technology available in the market (Olushola & Abiola 2017; Sabi, Uzoka, Langmia & Njeh 2016; Rahayu & Day 2015). The proponents of the TPB view technology adoption as being influenced by an individual's behavioural, normative and control beliefs about the benefits of the technology (Olushola & Abiola 2017; Akinbi 2015; Ajzen 1991).

Firstly, it is assumed that *behavioural beliefs* can compel an individual to assess the desirability of the outcomes of adopting and using the technology (Bach et al. 2016; Wisdom, Suite & Horwitz 2014). This means that decision-makers in SMEs can adopt and use Cloud BI after evaluating the benefits and risks of the business operations. However, a successful evaluation depends on knowledge about applications, how they work, and the benefits and risks associated with their use (Hamida et al. 2016; Meijer, Catacutan, Ajayi, Sileshi & Nieuwenhuis 2015; Wisdom et al. 2014; Horst, Kuttschreuter & Gutteling 2007).

Secondly, *normative beliefs* are perceived social pressures from peers and competitors that can influence an individual to consider adopting and using new technologies (Fry et al. 2018; Sniehotta, Presseau & Araújo-Soares 2014; Williams & French 2014). According to Horst et al. (2007), the potential adopter can be influenced by the opinions of other users about the technology. Therefore, normative beliefs can cause an individual to act either rational or irrational towards a new technology (Williams & French 2014; Ajzen 1991). A rational behaviour involves the individual evaluating the benefits and risks inherent in the technology (Momani & Jamous 2017; Horst et al. 2007; Ajzen 1991), while irrational behaviour refers to when an individual adopts a technology due to social peer pressure at the expense of the needs of the enterprise (Taherdoost 2018; Hamida et al. 2016). The implication is that decision-makers need to be very cautious about the benefits and risks of Cloud BI and should desist from adopting technology without due diligence.

Finally, *behavioural control beliefs* refer to the perceived easiness or difficulty of using the technology to produce desirable results (Fry et al. 2018; Taherdoost 2018; Williams & French 2014; Wisdom et al. 2014). The knowledge and skills needed to use new technology are reported to be more influential on the adoption than the benefits that enterprises can derive (Fry et al. 2018; Meijer et al. 2015; Renny, Guritno & Siringoringo 2013). This means that potential adopters tend to assess how easy-to-use an IT application is and overlook other important aspects, including security (Afolayan & de la Harpe 2019; Afolaranmi et al. 2018; Clohessy 2017; Renny et al. 2013). The TPB shows that the manner in which individuals choose technology can be influenced greatly by beliefs regarding the favourableness or unfavourableness of the outcomes of using the technology (Olushola & Abiola 2017; Sniehotta et al. 2014).

Implicitly, the TPB encourages SMEs to engage in planning, assessing, and evaluating the technology for possible benefits, risks, and usability before its adoption. SME decision-makers constantly make decisions on the operations that affect the course of business, which may have possible consequences on the success of the business. The decision to adopt and use Cloud BI relies on whether decision-makers perceive that technology can improve enterprises, regardless of other circumstances. Besides benefits, decision-makers can decide to adopt and use Cloud BI to match their competitors even though they may not realise many benefits, as long as they are keeping up with technological trends. Decision-makers have limited time to learn how to use technology, and as such, any technology perceived to be difficult to learn has little chance of being adopted and used. Concerning South African SME decision-makers, the level of awareness and interest in Cloud BI and other technologies are well documented (Mohlameane & Ruxwana 2014; Moore 2014; Dawson & Van Belle 2013; Modimogale & Kroeze 2009). According to Bam and Adao (2019), SME decision-makers fear the backlash from making wrong decisions on the choice of IT solutions to invest in.

However, TPB does not provide guidelines on how individuals can evaluate technology to accomplish the adoption process, hence the need to consider other theories. The TPB is more of an adoption theory than an evaluation theory. Several limitations to TPB have been discussed in many studies, and these have a bearing on this study. Generally, the TPB:

- assumes that an individual always has a chance and the resources needed to successfully perform the desired behaviour, regardless of the intention (Miller 2017; Tan et al. 2015; Sniehotta et al. 2014; Williams & French 2014);
- does not clearly explain the effects of variables such as anxiety, hazard, attitude or previous experience as characteristics of behavioural intention and motivation (Williams and French, 2014; Miller, 2017);
- overlooks environmental and economic factors that can influence a person's intention to behave in a certain manner regarding a new technology (Sniehotta et al. 2014; Miller, 2017);
- assumes that behaviour is a consequence of a prearranged and easy decision-making process that does not change for a long time (Miller 2017);

- assumes that an individual does not have control over one's behaviour (Sniehotta et al. 2014; Williams & French 2014); and
- fails to forecast the time interval from the intent and behavioural action (Miller 2017; Sniehotta et al. 2014; Williams & French 2014).

## ii. Technology Acceptance Model

Similar to TPB, the Technology Acceptance Model (TAM) emphasises perceived usefulness (PU) and perceived ease-of-use (PEOU) of technology as the most influential factors in the adoption process (Venkatesh et al. 2018; Momani & Jamous 2017; Olushola & Abiola 2017; Bach et al. 2016). Based on the TAM, the intentions of enterprises to adopt IT products and services depend on their PU and PEOU of using the technology to solve business problems (Hamida et al. 2016; Horst et al. 2007). Implicitly, enterprises are inclined to adopt and use a technology perceived as being useful and easy-to-use. Some studies used TAM to predict the uptake and continuation of the use of different technologies (Venkatesh et al. 2018; Momani & Jamous 2017; Senarathna et al. 2016; Horst et al. 2007).

The TAM has been criticised for being unsuitable in explaining technology adoption in enterprises but is suitable for the acceptance and use of technology at a personal level (Ajibade 2018; Lai 2017). For example, separate studies by Ajibade (2018) and Chandio, Burfat, Abro and Naqvi (2017) allege that the TAM cannot be used to explain why users adopt and use new technology such as e-government despite its popularity. Another criticism of the TAM is for being inconsistent in explaining the behaviour of users when buying, accepting and rejecting a new technology (Devesh et al. 2017; Hai & Alam-Kazmi 2015). It is reported that the TAM does not consider the evaluation of risks because it focuses more on the benefits and usefulness of technology (Hamida et al. 2016; Horst et al. 2007). Wu (2012) points out that the TAM, popularly used in technology adoption research, does not explain how the PU and PEOU could be practically assessed. Ideally, the TAM is an acceptance model suitable for dealing with attitudes and beliefs and falls short of explaining the challenges in the adoption of technology from a pragmatic perspective.

### iii. Diffusion of Innovation Theory

The Diffusion of Innovation Theory (DoIT) explains the adoption of innovations in terms of benefits and risk factors, such as lack of knowledge, relative advantage, trialability, compatibility and complexity of the innovations that increase uncertainty (Ren 2019; Sadoughi, Ali & Erfannia 2019; Sahin 2006). The fact that some social groups are more eager to adopt a technology than others means that the innovation will be adopted differently in different societies (Osorio-Gallego, Londono-Metaute & Lopez-Zapata 2016; Salim, Li, He & Shen 2016; Haji, Mohd & Abd 2015). Besides the benefits and risks of technology, the characteristics of the enterprise are regarded as being influential in terms of the technology adopted (Fry et al. 2018; Lai 2017; Rogers 2005). This is seen in the DoIT categorising enterprises as innovators, early adopters, early majority, late majority and laggards based on the unique characteristics of each group, which is thought to affect technology adoption tendencies (Rogers 2003, 2005; Salim et al. 2016; Salim et al. 2015).

Studies that implemented the DoIT describe *Innovators* as opportunistic adopters and non-evaluators of an innovation (Taherdoost 2018; Hayes, Eljiz, Dadich, Fitzgerald & Sloan 2015). They are eager to exploit the technology at its inception and are willing to manage unbeneficial and unproductive innovations; and are prepared to accept a certain level of risk about the innovation (Clark 2012; Rogers 2005). SMEs are least likely to be innovators due to several challenges they might face in the quest to adopt new technologies. The early adopters, early majority and late majority adopt technology supposedly after assessing benefits and risks (Ajibade 2018; Wisdom et al. 2014; Evens, De Marez & Schuurman 2008). The degree of evaluation increases from early adopters to the late majority (Fry et al. 2018; Clarke 2012). These groups of adopters base their evaluation on the experiences and opinions of innovators, which may give wrong impressions, resulting in inappropriate decisions being taken. The DoIT illustrates that the evaluation of technology before its adoption is very important but does not provide how the evaluation could be done. For this research study, it is appropriate to collect data that might provide insights into the realities of the practices of SMEs in small South African towns.

Based on the DoIT, SMEs may avoid adopting an innovation because of the undesirable consequences it brings about and the fear of business risks among decision-makers who cannot deal with the consequences (Ren 2019; Sahin 2006). Thus, the literature suggests that the adoption

of Cloud BI by SMEs is more likely to be influenced by risks than benefits (Beever 2018; Lai 2017). This means that negative consequences, such as security breaches, loss of revenue, and tarnishing of the image of the enterprise, may have a detrimental impact on the adoption of available Cloud BI. To reduce the risks of adopting innovation, decision-makers need to have enough knowledge of the benefits and risks of the innovation before the adoption (Peltier, Zhao & Schibrowsky 2012; Oliveira & Martins 2011). This can be alleviated by evaluating Cloud BI to identify risks and threats in the technology that CSPs could not have disclosed to the decision-makers.

The DoIT is criticised for its failure to evaluate innovations from the perspective of end-users because it assumes that the adoption of innovation is always a desirable undertaking (Lai 2017; Osorio-Gallego et al. 2016). Furthermore, the theory disregards the experience and challenges faced by adopters because of its assumption that all information about the innovation is available. It could be observed that the DoIT does not provide for a systematic evaluation of innovation due to its over-simplification of the adoption process by focusing on discrete technical changes by individuals and groups.

#### **iv. Multi-stage adoption models**

The Multi-Stage Adoption Model (MSAM) suggests five stages of a decision-making process when an enterprise decides to adopt an innovation (Ettlie 1980). The evaluation and trial stages, which can be merged into a single stage, occupy most of the decision-making process, and therefore, are the most important stages of the adoption process (Salim et al. 2015; Thong 1999; Ettlie & Penner-Hahn 1994). The advantage of the MSAM is its closeness to the process of technology adoption used in industry and deals with the reality on the ground (Salim et al. 2015; Ettlie & Penner-Hahn 1994). Both the evaluation and trial stages can enable an enterprise to assess the benefits and risks of the new technology. Similar to the DoIT, the MSAM emphasises the importance of information about the benefits and risks of the technology, which is needed to make decisions about adopting the technology (Igli & Solange 2019; Osborn 2014). Information about the new technology can be obtained from various sources during the evaluation process.

*Awareness* is the stage whereby decision-makers recognise the existence of a useful technology that can be used to address a need or solve a business problem (Sadoughi et al. 2019; Ettlie &

Penner-Hahn 1994). Three forms of knowledge, important for the successful adoption of an innovation, are identified as awareness knowledge, how-to-knowledge, and principles-knowledge (Osborn 2014; Sahin 2006; Rogers 2005). The *awareness-knowledge* is acquired when the potential adopter comes to know about the existence of the new technology; the *how-to-knowledge* pertains to how the technology can be used correctly; and *principles-knowledge* describes how and why an innovation works (Rogers, 2005; Sahin, 2006). Limited how-to-knowledge and principles-knowledge may hinder the adoption and use of new technology. Enterprises adopting new technologies with limited how-to-knowledge may misuse the technology and risk producing unintended results, which lead to premature discontinuation. In South Africa, the increase in the utilisation of smartphones, social media platforms and the open web has exposed SME decision-makers to a variety of information sources, such as peers, business partners, competitors, and CSPs, directly or indirectly (Small Enterprise Development Agency 2020; Iqbal et al. 2016; Osborn 2014). This can increase the three forms of awareness knowledge.

The *interest stage* involves decision-makers actively searching for information about specific technology and its possible substitutes (Salum et al. 2016; Salim et al. 2015). The potential adopter wants to know where to acquire the technology, learn how it works, who should use it and system specifications (Salim et al. 2014; Ettlie 1980). There is a possibility that the individual would want to be acquainted with the technology to see features and learn how they work. To reduce the uncertainty about the technology the potential adopter tends to seek the benefits and risks, which initiates the evaluation and trial stages. These days, several websites provide information about Cloud BI, which can easily be accessed timeously. However, evaluating the authenticity of information is essential.

The *evaluation stage* involves many activities intended to provide information about the technology and an opportunity for potential adopters to learn much about the new technology (Ettlie & Penner-Hahn 1994; Ettlie 1980). The evaluation involves the systematic gathering of data and analysing of information, assessment of the new technology by comparing benefits and risks with other existing technologies (Salim et al. 2015; Rogers 2005; Ettlie 1980). In conventional IS, the evaluation stage tends to be the longest in the adoption process because several activities need to be completed, including thorough inspection and pretesting of the technology before a decision



to adopt is made (Tripp, Pistoia, Cousot, Cousot & Guarnieri 2013). Cloud BI can be evaluated in terms of benefits, functionalities, financial and security risks, data confidentiality, integrity and availability (CIA) and CSPs characteristics (Senarathna et al. 2016; Chou 2013). The evaluation stage is tedious and decisive in the technology adoption process, and as a result, several potential adopters may fail to complete it due to the challenges they face.

The *trial or testing stage* of the MSAM involves an enterprise making an effort to use the technology on an experimental basis to check if its utilities were fully deployed (Salim et al. 2015; Ettlíe & Penner-Hahn 1994). Although the technology is being used on a limited basis, the results or output can be used to improve business decision-making processes. Concerning Cloud BI, SMEs can benefit from using free versions of the application from the web which, can be used for a given duration of time without upfront payment. The purpose of the trial stage is to allow the potential adopter to use the free service to understand how the new solution works and how it can be integrated with existing business systems or processes (Salim et al. 2014; Phneah 2013). According to Budrienė and Zalieckaitė (2012), an enterprise can conduct tests with different applications, then compare results to select the most appropriate solution.

For a potential adopter to proceed to the evaluation and trial stages, the interest in the adoption should be sustained. The evaluation and trial stages can provide important information that can be used to confirm or refute the PU and PEOU of Cloud BI, thus, preventing decision-makers from making mistakes in either adopting or rejecting the technology on an unfounded basis. Literature indicates that it is highly likely that an enterprise can adopt new technology before evaluating and testing to check whether it is useful or risky based on the opinions of other potential adopters (Taherdoost 2018; Olushola & Abiola 2017). Enterprises that seek to reduce uncertainty prefer to evaluate and test the technology before adoption it (Kazmi, Ghani, Mohamad & Tariq 2016; Gupta & Kaur 2013). This tells us that the MSAM focuses much on the technology and disregard other factors, such as the environment in which the technology is used.

*Commitment* is the last stage in the MSAM adoption process, comprising of the adoption and implementation of the technology (Salim et al. 2014; Ettlíe 1980). This takes place when decision-makers are satisfied that the technology meets the requirements and expectations of the enterprise.

#### **v. Important takings from the technology adoption theories**

The literature from technology adoption theories suggests that enterprises are influenced by several factors on whether to adopt or reject new technology. The TAM emphasises the perceived benefits of the use of technology (Horst et al. 2007); the TPB stresses both the benefits and risks of adopting a technology (Taherdoost 2018; Olushola & Abiola 2017). The DoIT stresses risk factors related to lack of knowledge, trialability, compatibility, and complexity of the new technology (Lai 2017). However, the DoIT brings in the dimension of the characteristics of different technology adopters which influence the adoption process. This literature highlights the difficulties in the process of adopting new technologies and points to the need for potential adopters to conduct proper evaluations.

#### **vi. The gap in theories of technology adoption**

The existing body of IS research on the adoption of new technologies is highly influenced by adoption theories and limited in-depth on how SMEs can evaluate various technologies before their adoption, regardless of several frameworks and models purporting to aid these enterprises. The problem lies in the failure of discriminating between SMEs and LBEs' business, process and technological needs (Boonsiritomachai et al. 2014; Jelonek & Wysocka 2014). This has resulted in many studies prescribing frameworks and methodologies for cloud computing technologies adoption to SMEs in different economic sectors. The TPB and TAM deal with attitudes and beliefs towards technology and ignore important aspects, such as the service providers and the environment in which the technology is used. These theories cannot explain disparities between the adoption of technologies for personal and enterprise use in SMEs in which businesses are run along personal lines. The DoIT suggests core aspects that can be influential to the adoption of the technology but fails to explain how the assessment process can be successfully conducted. The MSAM provides fundamental explanations of the adoption process as stages. However, it is not a security evaluation framework because it does not provide guidelines for checklists to be used.

#### **2.5.2. Benefits of Cloud business intelligence as enabling factors to adoption**

The use of IT business solutions has a profound effect on the market environment, service provision, business operations, consumer behaviour, and decision-making on how enterprises

should operate in a digital economy (UK Essays 2018a; Olszak 2014; Ong et al. 2012; Zembylas & Vrasidas 2005). A digital economy, a segment of the knowledge economy, is characterised by the use of digital computing technologies to access, process, manage and communicate information by business enterprises, government, and community members (Mabotja 2019; Hretcanu 2015).

Several documented characteristics of Cloud BI depend on cloud computing (Columbus 2018; Indriasari, Prabowo, Meyliana & Hidayanto 2018; Agostino et al. 2013). Due to this dependency, some literature sources provide blurred differences between the characteristics of Cloud BI and cloud computing (Gurjar & Rathore 2013). According to the TPB and TAM, the perceived benefits that the technology is supposed to bring to the enterprise can promote its adoption (Sadoughi et al. 2019; Taherdoost 2018; Olushola & Abiola 2017; Hamida et al. 2016). The DoIT asserts that the relative advantage, which is a cluster of benefits of new technologies over the existing one, can influence enterprises to adopt and use the new technology (Hayes et al. 2015; Greenhalgh, Robert, Macfarlane, Bate & Kyriakidou 2004; Thong 1999). According to Lai (2017), for an innovation to be adopted, it must provide more tangible benefits to the one being used. This implies that an enterprise can adopt a technology if it improves competitiveness and viability. Several supposed benefits, which influence SMEs to adopt Cloud BI, are well documented. Such benefits include data visualisation, usability, and financial benefits.

#### **i. Data analysis, visualisation, and reporting**

Data analysis and visualisation are Cloud BI features for analysing data and presenting results in formats that are simple for standard users to interpret and make implementable decisions without involving data analytics experts (Senarathna et al. 2016; Agostino et al. 2013). SME decision-makers seldom make decisions from the data they generate (Boonsiritomachai et al. 2014; Lacey & James 2010). Therefore, the use of data analysis and visualisation tools in Cloud BI may assist SME decision-makers to develop habits and confidence in analysing data on their own to improve operational decision-making.

Similarly, a Cloud BI provides *reporting* tools for easy data upload; and to create reports, displayed on interactive easy-to-use dashboards, for standard users without business analytics knowledge (Phocas Software 2015; Menon et al. 2012). Reports and dashboards have added the business value

of being easily accessible over the web on a wide range of devices, such as smartphones and desktops, at a comparably low-cost pay-per-use facility (Columbus 2017, 2018; Patel & Connolly 2007). The potential benefits of Cloud BI can dispel the doubts cast by Boonsiritomachai, McGrath and Burgess (2014) on whether SMEs could realise the potential business value in their data because of a lack of suitable technologies to assist them to achieve data management for decision-making.

## **ii. Decision-making**

Studies show that most SME decision-makers struggle to make the correct decision timely because they still depend on manual or traditional IS (Papachristodoulou et al. 2017; Brezinova 2013). This makes decision-making in SMEs a cumbersome process, marked by a lack of accurate and up-to-date information (Kasem & Hassanein 2014; Nyalungu 2011). The weaknesses of conventional IS are evident in the inability of decision-makers to manage large volumes of data to get quality information needed for decision-making. Cloud BI provides data analysis and visualisation facilities that can enable decision-makers to process data, display results visually, and generate reports in a meticulous way suitable to their business needs (Patil & Chavan 2020; Elmalah & Nasr 2019). Unlike traditional BI, Cloud BI can be used by standard users to speedily produce accurate reports for decision-making purposes (Phocas Software 2015; Kasem & Hassanein 2014; Olise, Anigbogu, Edoko & Okoli 2014). Nonetheless, the adoption and use of Cloud BI does not translate to instant benefits but require the proper use of the technology, guided by business objectives (Herwig & Friess 2016; Thompson & van der Walt 2010). Decision-makers need to seriously consider if the adoption of Cloud BI can add value to their decision support systems.

## **iii. Knowledge about market trends and economic activities**

Cloud BI is reported to help provide enterprises with a depth of knowledge about market trends, economic activities, and internal operations crucial for effective and good quality business decision-making (de Jongh, Janette Larney, Mare, van Vuuren & Verster 2017; Ranjan 2014). SMEs are expected to use Cloud BI to create an informational space, to analyse operational data. This will allow SME decision-makers to see key strategic business dimensions which are important in monitoring consumer patterns (Agostino et al. 2013; Bucur 2012). Another justification for

using Cloud BI is the claim by Gendron (2014) that they have the potential to transform the role of decision-makers from information consumers to producers. This shows that the usefulness of Cloud BI in determining the market trend and economic activities can improve the viability of SMEs in small South African towns. The limitation is that decision-makers may not be prepared to share information with their competitors due to fear of loss of customers.

#### **iv. Improving customer care**

Customer services, a major source of revenue, is another area where SMEs are reported to be lacking, and this can influence the need to adopt and use Cloud BI (Koparkar & Mackrell 2015; Mashingaidze 2014; Scholz et al. 2010; Olszak & Ziemia 2004). SMEs' managements need information that enables them to conduct a variety of activities in the enterprise, by creating new methods of co-operation, attracting new customers, creating new markets, and offering the right solutions to customers (Chou 2013; Olawale & Garwe 2010). Cloud BI is reported to be useful in developing a customer-centric approach for easy tracking of customer contacts and monitoring issues they raise (Kasem & Hassanein 2014; Gurjar & Rathore 2013). Persistent competition for customers makes it imperative for SMEs to consider utilising Cloud BI to manage online communication channels to listen to customer compliments, needs, and complaints (Brooke 2019; Sharda, Delen & Turban 2015). Customer care can be improved by using Cloud BI to create portals for customers to easily monitor their business and social activities, and access information about new merchandise and bills (Schiff 2016; Chou 2013). Ultimately, improving customer experience can reduce customer dissatisfaction.

#### **v. Professionalism in information analysis**

A study by Turyakira (2018) claims that SMEs lack professionalism because they are often run by owners or family-appointed managers who do not realise the importance of using proper data management tools. Olexova (2014) posits that SME decision-makers need to improve professionalism in the acquisition and analysis of information by utilising Cloud BI. According to Ranjan (2014), proper use of Cloud BI can reduce the tendency of SMEs to use trial-and-error techniques when making important decisions, but instead use accurate reports to respond timely to financial conditions, customer preferences and supply operations. By using Cloud BI, SMEs are expected to effectively deploy their practices, processes, and technology to create a sound

knowledge base to support their business units (Dawson & Van Belle 2013; Olbrich, Poppelbus & Niehaves 2012). The need to improve professionalism can influence SMEs to adopt and use Cloud BI.

**vi. Usability of Cloud business intelligence**

Unlike traditional IT and BI applications, which demand considerable training, Cloud BI can relieve decision-makers from this type of learning because it offers easy training for application use only (Kyobe, Namirembe & Shongwe 2015; Dawson & Van Belle 2013). In this context, Cloud BI can empower ordinary SME decision-makers with basic IT knowledge so that they can actively participate in the digital revolution and improve the way business services are provisioned and expended (Patil & Chavan 2020; Chin, Callaghan & Clarke 2008). This raises optimism that decision-makers may no longer be constrained from adopting and using Cloud BI by a lack of technical skills, which are no longer a prerequisite for using these applications (Worku 2013; Chin et al. 2008). However, similar to other IT solutions, decision-makers would have to evaluate each Cloud BI to select the most appropriate and learnable application to suit their needs.

The DoIT postulates five qualities of an innovation that can influence its adoption, namely compatibility, complexity, trialability, observability, and relative advantage (Beever 2018; Hayes et al. 2015; Greenhalgh et al. 2004). These qualities are important when evaluating Cloud BI.

*Compatibility* is the extent to which new technology can integrate with the existing values, past experiences, and needs of potential adopters (Elmalah & Nasr 2019; De Jongh et al. 2017; Hooda 2014). A study by Greenhalgh et al. (2004) suggests that an innovation compatible with the existing enterprise system has a higher chance of being considered for adoption. There are claims that Cloud BI can be integrated into existing enterprise systems, data sources, and other clouds easily (Elmalah & Nasr 2019; Wisdom et al. 2014; Ereth & Dahl 2013). However, data portability and cloud interoperability are widely regarded as some influential factors that enterprises consider before the adoption of Cloud BI (Ren 2019; Osorio-Gallego et al. 2016; Carcary et al. 2014; Thong 1999). These can prevent SMEs from adopting Cloud BI, fearing data corruption during conversion.

*Complexity* is the quality of a technology used to describe how demanding it is to understand and learn the new technology (de Jongh et al. 2017; Thompson & van der Walt 2010). According to Rogers (2005), new technologies perceived as complex have a low chance of adoption and use compared to those perceived as simple (Hayes et al. 2015). Cloud BI has been touted as being simple and easy to learn and that users could be able to use tutorials by themselves instead of taking lengthy formal courses or workshops (Patil & Chavan 2020; Senarathna et al. 2016). This emphasises the importance of decision-makers evaluating the complexity of each Cloud BI before adopting it.

*Trialability* is important when deciding to adopt an innovation. Potential adopters of new technologies are influenced by *trialability*, the extent to which an innovation can be tried out with limited use in the enterprise (Lai 2017; Osorio-Gallego et al. 2016). Before investing money, effort, and time into new technology, enterprises should try to implement it. From this literature, it is clear that technologies that can easily be tried, have a higher chance of being adopted. There is overwhelming evidence that Cloud BI can easily be tried by a standard IT user (Beever 2018; Hayes et al. 2015; Keesee & Shepard 2011), and this can influence decision-makers to consider adopting the applications.

*Relative advantage* has been defined as the extent to which an innovation is perceived as being better than the one it will replace (Rogers 1995, 2003). Technology relative advantage can be understood in terms of several benefits including economic profitability, social prestige or competitive advantage (Mairura 2016). SMEs considering the adoption of an IT solution are encouraged to consider if the technology can solve problems being experienced or provides alternative business opportunities that lead to the enterprises improving productivity and operational efficiency to survive economic challenges (Balachandran & Prasad 2017; Mairura 2016; Mndzebele 2013).

According to the DoIT, all potential adopters, except innovators, depend on *observability*, the extent to which the outcomes of an improvement are visible to the enterprise (Beever 2018; Hayes et al. 2015; Keesee & Shepard 2011). This implies that individuals intending to adopt an innovation usually seek tangible benefits of the technology before deciding to adopt it. According to Hayes *et*

al. (2015), positive observable outcomes when using new technologies can influence their adoption. This highlights the need for enterprises to desist from adopting new technologies based on marketing information because marketers may exaggerate the benefits of innovations.

Further benefits of using cloud computing technologies cited in recent studies include security, elasticity and scalability, on-demand, availability, and mobility.

*Security* is an essential benefit debated by those who encourage SMEs to adopt and use cloud services (Patil & Chavan 2020; Elmalah & Nasr 2019; Salim et al. 2015). This emanates from the claim that CSPs are responsible for securing cloud computing technologies while the clients secure their data and applications (Columbus 2017, 2018; Al-Aqrabi et al. 2015). In an ideal situation, the cloud should be more secure than on-premise information assets because the CSPs are specialised in security (Salum et al. 2016; Alia, Khana & Vasilakos 2015). There are mixed views regarding security in cloud computing technologies and the environment in which they are used, and these may ultimately affect security in Cloud BI (Bilal, Malik, Khan & Zomaya 2014). SME decision-makers should evaluate security in the cloud and CSPs before adopting the technology, as recommended by Hatwar and Chavan (2015) and Harrison et al. (2016).

*Elasticity and scalability* of cloud computing technologies make Cloud BI flexible as they can be scaled up and down dynamically with the changing needs of the SMEs (Gurjar & Rathore, 2013; Sherman, 2015). A survey on the adoption of Cloud BI by Columbus (2017) reports that elasticity and scalability are among the main reasons for SMEs to adopt and use Cloud BI. This assertion shows that SMEs can benefit from the flexibility of Cloud BI by using the technology periodically in a limited manner while paying for the functionality they use. For SMEs to benefit from the flexibility of Cloud BI, decision-makers should be able to select the appropriate application, which requires proper evaluation. However, reports on uncertainties about the flexibility of Cloud BI on offer justify the need for decision-makers to evaluate cloud services before adoption (Heang 2017; Agostino et al. 2013).

*On-demand, availability and mobility* mean that Cloud BI brings about convenience to decision-makers in accessing applications and managing data remotely on their mobile devices over the



web (Hurtaud & de la Vaissière 2017; Menon et al. 2012). This makes it easy for decision-makers to manage enterprise information wherever they will be, without worrying about accessibility, proximity, system speed, or effectiveness (Elmalah & Nasr 2019; Columbus 2018; Shukla, Agarwal & Shukla 2012). In the context of South African SMEs in remote small towns, it is risky to assume that all enterprises have reliable Internet connectivity and that all CSPs offer the same level of trust and performance. Secondly, conducting transactions over unsecured web services and management interfaces have security implications that need to be addressed (Salum et al. 2016). SMEs can easily be victims of cyber threats, such as hackers who commit security breaches in the cloud (Barhatov, Campa & Pletnev 2017). This further justifies why SMEs should consider the evaluation of Cloud BI as an important process to undertake.

#### **vii. Financial benefits**

Some studies indicate that Cloud BI can enable SMEs to reduce overhead costs and save money by reducing the number of on-premise IT resources and IT staff needed to manage daily operations compared to traditional BI (Columbus 2017; Phocas Software 2015; Sherman 2015; Vasista 2015). It is further alleged that enterprises only need to configure the front-end of the Cloud BI software free of charge or at a nominal cost (Columbus 2018; Kasem & Hassanein 2014). Cloud BI can easily be configured by standard users, which reduces the costs of hiring IT specialists (Columbus 2018; Dresner 2017; Walczak 2014). Enterprises who opt to adopt Cloud BI do not incur any costs for infrastructure installation, deployment, maintenance, servicing updates, improvements, or trouble-shooting because these are administered by the CSP off-premises (Columbus 2020; Kaur, Azad & Singh 2013; Shukla et al. 2012). This implies that SMEs with small financial budgets will be able to access BI services from the cloud at a low cost. However, cost reduction is debatable due to a few issues related to hidden costs and litigations over breach of privacy (Ghaffari et al. 2014). Therefore, this makes it prudent for decision-makers to evaluate Cloud BI to avoid financial risks.

The benefits of utilising Cloud BI are improving the competitiveness and viability of SMEs in small South African towns because they can enable a reliable analysis of data to provide results for decision-making on enterprise operations and future investments (Herwig & Fiess, 2016; Olise, Anigbogu, Edoko, & Okoli, 2014). The fact that the benefits do not translate to the successful

adoption of Cloud BI by SMEs in South Africa is an indication of underlying issues that these enterprises face, which are worth investigating. The critics of the adoption and use of Cloud BI claim that the technologies are inherently less secure and can expose an enterprise's data and information assets to security threats (Indriasari et al. 2018; Jelonek & Wysocka 2014). This notion is affirmed by Kasem & Hassanein (2014), who posit that security remains an exceptional challenge in cloud systems, particularly in public clouds where most of the data transactions are managed over the web. Besides relying on benefits, SMEs should be able to evaluate Cloud BI to establish whether they meet their business and security expectations, and risks associated with the technology used.

### **2.5.3. Characteristics of small and medium enterprises**

A few studies conducted in South Africa on the adoption and use of cloud services show that it follows the same trends as elsewhere in the world. For example, Mohlameane and Ruxwana (2014) report improved awareness of cloud computing technologies among SMEs in South Africa; Lechesa, Seymour and Schuler (2012) highlight the challenges affecting the willingness of South African SMEs to adopt cloud services. Mashandudze and Dwolatzky (2015) indicate that SMEs cannot adapt and use Cloud computing technologies because this may result in their short life span. However, most of these studies focused more on the awareness and perceived usefulness of the technology and provide solutions that are best suited for users with expertise in IT.

*Knowledge* about innovation and how it is used is regarded as an important determinant of technology adoption (Lai 2017; Osorio-Gallego et al. 2016; Nyoro et al. 2015). The advent of cloud services has revived the research regarding the effect of knowledge of the potential adopter on the adoption of these technologies (Rupra, Karie & Rabah 2018; Elena & Johnson 2015a; Osborn 2014). Such studies are influenced by the TPB and DoIT, which emphasises the importance of knowledge and skills in using cloud computing technologies (Ren 2019; Sadoughi et al. 2019; Hamida et al. 2016; Yauri & Abah 2016; Nyoro et al. 2015). In SMEs, decisions are mainly made by the owners or managers who have limited technical knowledge and skills to use Cloud BI to improve decision-making (Papachristodoulou et al. 2017; Brezinova 2013). Such decisions can be based on the individual SME decision-maker's past experiences (Papachristodoulou et al. 2017), and/or opinions of other users about the technology (Fry et al.

2018; Hamida et al. 2016; Horst et al. 2007). According to Sadoughi, Ali and Erfannia (2019), limited knowledge about Cloud BI and how they work raises many uncertainties among decision-makers. This implies that limited knowledge of how to use Cloud BI and how they could improve operations can lead to uncertainty and mistrust by decision-makers. A study by Khan and Al-Yasiri, (2015) asserts that SMEs should have adequate knowledge about cloud computing technologies before they start thinking about adoption. This confirms that lack of essential knowledge can be an influential factor that negates the adoption and use of Cloud BI by decision-makers, regardless of their awareness of the benefits (Papachristodoulou et al. 2017; Ibrahim & Musah 2015).

Furthermore, a survey on small manufacturers and financial services organisations conducted in the United States of America by Chao and Chandra (2012) reports that the SME owner's level of IT knowledge is a key determinant of IT strategic alignment and adoption of Cloud BI. This illustrates that good knowledge of Cloud BI by SME decision-makers is important in the adoption and use of technology. However, Dholakiy (2016) posits that Cloud BI is designed to be used by individuals with basic IT skills who may not need to undergo advanced training. These findings may be important in indicating the different types of IT knowledge that decision-makers should have to adopt and use Cloud BI.

Recent studies suggest that the adoption of Cloud BI should be informed by current and accurate information about the operational and security benefits of the applications (Patil & Chavan 2020; Mirai Security 2019; Olszak 2014). According to the DoIT, a lack of relevant information about the benefits and risks of innovation can hinder enterprises from adopting the technology (Fry et al. 2018; Lai 2017; Alshamaila et al. 2013). Some studies report that poor communication about new technology can cause decision-makers to rely on informal information, which leads to poorly documented strategic plans for IT use among SMEs (Brezinova, 2013; Kumar, Samalia, & Verma, 2017; Papachrisdoulou et al., 2017). Without correct information, decision-makers can face challenges in selecting Cloud BI due to the fear of making wrong decisions that may lead to risks, such as poor business performance and loss of customers (Brooke 2019; Schiff 2016; Sharda et al. 2015).

Connectedness is a key success factor in many business enterprises as they stay informed about market trends (Maguire & Delahunt 2017; Meijer et al. 2015; Salim et al. 2014). A study by Boonsiritomachai, McGrath and Burgess (2014) reports that SMEs lack connectedness to the outside world, including those already using IT, due to the fear of being exposed to their competitors. However, things have changed due to the use of social media technologies which make it easy for individuals to be connected outside their business spheres. This shows that the lack of knowledge about security evaluation among decision-makers can make them very conservative when conducting business because of their fear of the potential dangers of emerging technologies on their business operations. Furthermore, studies show that SMEs can only remain viable if they embrace and use emerging technologies for data management and decision-making (Malak 2016; Ghobakhloo, Sabouri, Hong & Zulkifli 2011). However, Timperley (2017) contends that adopting IT and getting connected to the Internet will never save SMEs as they have a small customer base due to poor connectedness.

#### **2.5.4. Security risk factors in cloud business intelligence**

The effects of security risks on the adoption of Cloud BI are documented in several Information Systems studies and will remain a topical issue in current and future research (Elmalah & Nasr 2019; Ereth & Dahl 2013). This indicates that decision-makers have to understand several security issues for the successful adoption and use of Cloud BI by SMEs, particularly those with basic security knowledge (Herwig & Friess 2016; Al-Aqrabi et al. 2015; Ashktorab & Taghizadeh 2012; Thompson & van der Walt 2010). A plethora of literature shows that security risks in cloud environments pose a major factor that militates against the adoption of cloud services by SMEs (Patil & Chavan 2020; Hooda 2014). Cyber threats in the cloud environment are reported to occur due to the vulnerabilities in the underlying cloud computing technologies used and in the cloud deployment models chosen (Cloud Security Alliance 2016; Mashandudze & Dwolatzky 2015; Fernandes, Soares, Gomes, Freire & Inacio 2014). The influence of these factors is confirmed separately by the TPB and DoIT perspectives with regards to risks and uncertainties influencing the adoption of various technologies.

**i. The vulnerabilities in the underlying cloud computing technologies**

Security vulnerability refers to an exploitable weakness in software or hardware that malicious attackers can use to penetrate computer systems to steal data, take control of the system or disrupt essential operations and services (Mogull, Arlen & Gilbert 2017; Fernandes et al. 2014). With the growing use of cloud services, security vulnerabilities have increased to the point that enterprises should have to increase their awareness about the types of flaws and the nature of their effects on personal life and businesses operations (Al-Aqrabi et al. 2015; Modi, Patel, Borisaniya, Patel & Rajarajan 2013). Unlike traditional IT applications, cloud applications are shareable among several clients, and any vulnerabilities in the technology can pose security risks in the clouds (Al-Aqrabi et al. 2015; Kumar & Padmapriya 2014).

According to Mashandudze and Dwolatzky (2015), SMEs fear the distressing effects of various cybersecurity threats and the risk on business viability. Thus, if they risk adopting and using Cloud BI without proper evaluation, it will affect their profits negatively. Understanding how these factors can influence SMEs in the uptake of Cloud BI is important in proposing a security evaluation framework for Cloud BI. Furthermore, Sangar and Iahad (2013) posit that security flaws in a Cloud BI depend on the cloud deployment approach being used. For example, the two common cloud deployment models, the public and community, which are accessible and affordable by SMEs, have vulnerabilities that can be exploited by cybersecurity threats and possibly lead to costly security risks to the information assets of enterprises (Patil & Chavan 2020; Venters & Whitley 2012). Ristov, Gusev and Kostoska (2012) assert that the weak security perimeter of both public and community clouds gives rise to security vulnerabilities that can easily be broken from the inside, leading to security breaches of information and data stored. This implies that knowledge about security in different cloud deployment models is important for SME decision-makers to make an informed judgement of Cloud BI before adopting and using the applications. Decision-makers are expected to be cautious of being victims of cyber threats and criminals who use security vulnerabilities in cloud environments to breach security in Cloud BI hosted in public and community clouds. Adopting Cloud BI without evaluating the underlying security flaws can be dangerous to SMEs where there is a lack of security specialists to assist when a security crisis arises. Studies by Agostino, Soilen and Gerritsen (2013) and Kazim and Zhu (2015) on cloud

computing security highlights the dangers of adopting cloud services and applications without due diligence.

Commonly cited vulnerabilities are those associated with user interfaces (UIs), Application Programming Interfaces (APIs), virtual networks (Mogull et al. 2017; Yauri & Abah 2016), and security configuration flaws (Cloud Standards Customer 2017). These vulnerabilities are technical and make Cloud BI susceptible to cyberattacks by hackers and malware (Majhi & Dhal 2016; Yauri & Abah 2016). Potential cloud adopters are unable to conduct a direct security evaluation on cloud infrastructure but can rely on information regarding security breaches provided by CSPs and publications in the special edition of security bulletins (Mogull et al. 2017; Yauri & Abah 2016). Reports on security breaches in Cloud BI show that vulnerabilities in UIs can be used as backdoors for bypassing normal authentication protocols (Symantec Corporation 2014; Chen & Zhao 2012). Regardless of the technical nature of the information, potential users of the clouds must be aware of the affected CSPs and how they mitigated the breaches. SMEs are encouraged to request reports proving that CSPs conduct successful penetration tests regularly and that the mechanisms are put in place to avoid similar breaches in the future (Salum et al. 2016; Carcary et al. 2014). However, some studies are sceptical about the preparedness of CSPs to provide such reports (Yu, Li, Hao, Li & Zhao 2017; Huang & Nicol 2013).

*Physical and environmental vulnerabilities* are due to defective physical access controls, improper siting of hardware, insufficient humidity and temperature controls, or malfunctioning electrical power systems for conditioners (Majhi & Dhal 2016). The Mirai Security (2019) argues that cloud services are exposed to similar security attacks and vulnerabilities that exist in the physical infrastructure where they are hosted. The inability of decision-makers to check the physical and environmental safety of their data may cause poor adoption of Cloud BI; due to the fear of losing data if physically unsecured hardware is damaged by natural causes or stolen.

A few studies report *operational vulnerabilities* as influential factors to Cloud BI, and this makes it important for decision-makers to understand these when adopting a cloud service (Jakimoski 2016; Lacity & Reynolds 2014). According to Senarathna et al. (2016), inadequate separation of cloud customers is a common operational vulnerability in enterprises where cloud services are

used. Decision-makers fear that sharing cloud services with other customers can make important data and processes vulnerable to deliberate or accidental deletion by users performing unauthorised operations (Ren 2019; Izrailevsky & Bell 2018). A study by Cobb (2014) observes that the lack of segregation of duties among employees of the CSPs can lead to unauthorised operations on customer data. This can negatively affect the adoption of Cloud BI by SMEs that use sensitive data.

*Security in the SaaS* layer is important in the adoption of Cloud BI because architecture differs among CSPs (Elena & Johnson 2015; Romes 2015). In SaaS, the major security problem is that enterprises have very little control over the applications and their data (European Union Agency for Network and Information Security 2015), which has been found to influence enterprises when adopting Cloud BI (Tiwari & Mishra 2012). Instead, SMEs usually depend on the security provided entirely by CSPs in Service Lease Agreements (SLAs), which define the conditions they operate under (Chou 2013; Hashizume, Rosado, Fernández-ME & Fernandez 2013). Enterprises are unable to ascertain whether the CSPs have put in place correct security mechanisms to protect data against security breaches in SaaS, but they depend on SLAs which might be challenging to understand.

SaaS is a multi-tenant service that enables different enterprises and users to store data in the same place (Afolaranmi et al. 2018; Fernandes et al. 2014; Subashini & Kavitha 2011). Security vulnerabilities in SaaS technology make it easier for clients to access each other's data and breach data confidentiality. This vulnerability can enable hackers who operate in SaaS to use unsophisticated methods to circumvent security controls and access sensitive data belonging to other clients (Akinbi 2015; Al-Aqrabi et al. 2015). This knowledge is vital to decision-makers during the evaluation process to determine whether CSPs would be accountable for legal liability in the event of a breach of data privacy.

*Data breaches* in cloud services continue to receive attention from cloud security researchers because they are among the most prevalent threats (Niselow 2018; Symantec Corporation 2014). According to Cloud Security Alliance (2016), data and application security breaches are defined as incidences in which unauthorised individuals release, view, steal or use an enterprise's sensitive,

protected, and confidential information intentionally or unintentionally. Ease-of-access of cloud services over web applications enables both inside and outside threats to commit data breaches in the cloud from outside and within the business enterprises (Akinola & Odumosu 2015; Chou 2013). A study by Khan and Al-Yasiri (2015) identifies malicious insiders and online cybercriminals as the major threats to most of the data breaches experienced by enterprises.

All the cited security threats bring about the critical security risks that SMEs would have to deal with for the successful use of Cloud BI (Takahashi 2018). This is enough evidence that cloud environments are not secure or immune to various data breaches including theft. SMEs have to proceed with caution in selecting Cloud BI and CSPs, which will provide the most appropriate security controls and reliable service at an affordable price. The question remains, how will SMEs conduct such an evaluation?

## **ii. Security threats and risks to cloud business intelligence systems**

A security risk refers to the possibility that a threat successfully exploits a vulnerability in an information system asset to disrupt the enterprise operations (Santos-olmo, Sánchez, Caballero, Camacho & Fernandez-medina 2016; Chang, Kuob, et al. 2015). Besides being aware of security vulnerabilities and threats, knowledge of possible security risks when migrating to the cloud is essential for decision-makers. The reason is that enterprises that fail to assess security risks in the cloud services they adopt are usually exposed to risks with severe consequences on the business operations and reputation (Devesh et al. 2017; Backes, Grimm & Kate 2016). Studies show that security threats and risks affecting each cloud delivery model always change and depend on the sensitivity of data and applications, architecture of the cloud, and security controls used in a particular cloud deployment (Elmalah & Nasr 2019; Pantić & Babar 2019). The following risks have been identified as prevalent in the SaaS service delivery model:

- *Privileged user access*: Literature shows that CSPs rarely provide proper controls to limit access to clients' data and information by their employees, which poses risks to the security and privacy of clients' sensitive data (Hussein & Khalid 2016). Loss of privacy may lead to litigation by customers and SMEs facing potential financial risks. Due diligence is needed when evaluating the cloud for access control features and UIs.



- *Data location and segregation:* Clients using public and community clouds hardly know where their data is being stored and hence lack complete control over it (Clohessy 2017; Hussein & Khalid 2016; Rivastava & Kumar 2015). The impending security risk is that data of different clients stored alongside each other can leak and mix up, compromising integrity and confidentiality (Cloud Security Alliance 2016). Although encryption is somehow effective, it cannot be the sole security means to provide the most reliable solution (Rupra et al. 2018; Yan, Ding, Yu, Zhu & Deng 2016). In some cases, cloud clients may not be interested in encrypting as they may be afraid that encryption accidents can destroy and make data irrecoverable (Hatwar & Chavan 2015). This security risk is important to SMEs to consider which data to store in the cloud.
- *Organisational security risks:* When a CSP shuts down business operations or gets taken over by another entity, clients are bound to suffer when changing to suit the new provider (Cloud Security Alliance 2016). Client enterprises will be required to migrate their data and applications to another CSP, thereby increasing the chances of exposure to malicious insiders who might breach data security and privacy (Subramanian & Jeyaraj 2018; Yan et al. 2016). Moreover, there is the possibility of data lock-in, which will limit the ability of the SME to retrieve its data from the collapsing CSP.
- *Physical security risks:* Client enterprises using public and community clouds depend on CSPs for the security of data centres to prevent unauthorised on-site access and theft of data (Cloud Security Alliance 2016; Yan et al. 2016). Firewalls and encryption are ineffective in protecting against physical data theft by CSPs employees. Clients have no idea of the location of their data or whether it is secure (Subramanian & Jeyaraj 2018; Yan et al. 2016).
- *Technological security risks* are due to hardware failure in the cloud, which leads to a CSP being unable to provide client enterprises with the essential services as agreed in the SLAs (Taherdoost 2018; Hussein & Khalid 2016). Multi-tenancy features of a public cloud pose challenges in separating resources shared among clients. This raises risks related to data and application portability when an enterprise decides to change to another CSP (Afolaranmi et al. 2018; Rupra et al. 2018; Hussein & Khalid 2016).

- *Compliance risks:* Data stored in the cloud are regulated by law in the country in which the CSP is located and should meet regulatory compliance (Mohlameane & Ruxwana 2020; Fernandes et al. 2014). Compliance risks arise when: 1) the CSP and clients do not have enough jurisdiction information governing electronic data issues; 2) there are changes in the jurisdiction which the CSP and clients are not aware of; and 3) the CSP has included illegal clauses to the contract likely to lead to legal disputes (Hussein & Khalid 2016; Fernandes et al. 2014). In some countries, the law makes it compulsory for CSPs to hand over sensitive information whenever the government makes such demands (Vitti, dos Santos, Westphall, Westphall & Vieira 2014). CSPs operating in such countries are expected to be externally audited and be granted security certifications that they can show to their clients (Potgieter 2019; Schaefer, Hofmann, Loos & Fettke 2014). Therefore, CSPs who do not undergo security compliance and audits raise mistrust among their clients, leading to avoidance of the adoption of the services.
- *Recovery risks* caused by failures in the cloud server can prevent data from being recovered (Mirai Security 2019; Vitti et al. 2014). In situations where a CSP fails to provide correct tools to restore all the data, service disruptions and loss of business occurs in an enterprise. Such risks arise when CSPs fail to meet their obligations stated in SLAs (Mesbahi, Rahmani & Hosseinzadeh 2018).
- *Long-term viability service* risk occurs when a CSP is bankrupt and shuts down services, is acquired by another CSP or merge with another business. This can bring about new policies that lead to cloud clients losing their data (Clohessy 2017). According to Hussain, Hussain, Hussain, Bagia and Chang (2018), CSPs place data in negative business conditions such as prolonged outages or flooding which makes it unavailable to clients leading to service disruptions.

There are several effects of security risks of adopting cloud services that point to the need to consider the effort of security evaluation by SME decision-makers before the adoption and use of Cloud BI by SMEs in disadvantaged small South African towns.

### **2.5.5. Cloud service providers**

CSPs play an important role by making infrastructure, platforms and services available to different users. Studies show that CSPs' characteristics, such as trust, reliability, performance, security, and pricing can promote or prevent the adoption of cloud computing by SMEs (Dresner 2017; Shimamoto 2015; Rostek et al. 2012). Normally, the CSP and client enterprises enter into service contractual agreements, Cloud service agreements (CSA) and Service lease agreements (SLA) that specify terms and conditions of service, including support, fees and rates, responsibilities and disclaimers (Cloud Standards Customer Council 2017; ENISA 2015). CSPs are always blamed for deliberately using problematic jargon in CSA and SLA that confuse potential clients (Cloud Industry Forum 2019; Yu et al. 2017). Without immediate assistance on contracts, SME decision-makers may find it difficult to understand the SLAs and this can hinder the adoption of Cloud BI and other cloud services (Akinbi 2015). This is further confirmed by Khan and Al-Yasiri (2015), positing that poor knowledge of SLAs among SME decision-makers is a challenge to the adoption of cloud services. The challenge that arises from SMEs' inability to interpret the contracts can lead to the mistrust of CSPs in delivering the service as promised (National Computing Centre Group 2018; Khan & Al-Yasiri 2015). This makes SMEs suspicious of being tricked by CSPs into signing contracts without due diligence (Yu et al. 2017; Zielinski 2009). However, decision-makers familiar with contracts are reported to be always suspicious of poor-quality cloud services that usually result in a financial loss when they try to correct them (de Jongh et al. 2017; Hussein & Khalid 2016). In the final analysis, decision-makers may not adopt Cloud BI due to mistrust of CSPs' security, reliability, and performance.

Furthermore, loss of data control to CSP when in the cloud, has been reported to be on the increase, particularly in the public cloud (Papachristodoulou et al. 2017; Hooda 2014). SMEs are reported to be afraid that once they lose data control to the CSP, they will be compelled to remain with the same provider for a long time (Senarathna et al. 2016). This leads to vendor lock-in, a security challenge reported in many studies on cloud services adoption by SMEs (Devesh et al. 2017; Agostino et al. 2013). Enterprises can be hesitant to adopt Cloud BI due to their fear of being trapped in one CSP for a long time (Cloud Security Alliance 2011). This fear can arise from the inability of CSPs to provide appropriate essential tools, techniques and standard data formats, services and interfaces which assure data and service portability (Opara-Martins, Sahandi & Tian

2016; Ereth & Dahl 2013; Rostek et al. 2012). Lack of service portability can restrict enterprises from switching to other CSPs offering better services and even switching from the cloud to on-premise systems (Durg & Podder 2020; Cloud Security Alliance 2016; Hussein & Khalid 2016). Vendor lock-in can be due to a CSP closing due to bankruptcy, leaving SMEs stranded with data locked in the defunct cloud.

Some reported data breaches in the cloud occur due to CSPs not being able to provide promised security and allowing their employees to conspire against certain enterprises for monetary benefits (Alliance 2015; Mahajan & Sharma 2015). A study by Khan and Al-Yasiri (2015) describes malicious insiders and online cybercriminals as the major threats that contribute to most of the data breaches experienced by enterprises. This is supported by Akinola and Odumosu (2015), who posit that employees at a CSP who have full access to the clients' resources hosted by the CSP, can access the data they are not authorised to. Although not all CSPs have such unethical employees, such reports of data breaches may influence SMEs to be very precautionous and prolong decisions on adopting Cloud services.

With several new CSPs in existence, it is becoming increasingly difficult for enterprises to determine which CSPs are genuine and capable of providing enough security to prevent data breaches and theft in SaaS. The benefits of SaaS applications can be outweighed by security threats posed by fake CSPs to whom an enterprise may lose control over their data.

#### **2.5.6. Financial risks**

One of the major purposes of SMEs is to generate revenue and make a profit (Small Enterprise Development Agency 2020; UK Essays 2018b; Widyastuti & Irwansyah 2018). Therefore, the use of Cloud BI should improve the profitability of SMEs. However, uncertainties in Cloud BI make SMEs fear the financial risks that can occur from many unprecedented security risks in the cloud (Ren 2019). South African SMEs are reported to be losing millions of rands due to data breaches that occur over cloud services (IBM Security 2020; Van Niekerk 2017; Gardner 2014). Although Cloud BI may enable SMEs to save finances, there are potential security risks and threats that may counteract these benefits (Elmalah & Nasr 2019; Patel & Connolly 2007) and these may constrain the uptake and use of technology in general. Abuse of computational resources has financial risk

implications because an enterprise can unknowingly use more paid resources than needed (IBM Security 2020; Van Niekerk 2017; Chang, Kuob, et al. 2015). Financial risks result from the combined effects of most of the other factors and can singly influence SMEs not to adopt Cloud BI.

## **2.6. Strategies used to evaluate cloud business intelligence**

Several studies apportion the blame for the slow uptake of cloud services by SMEs on a range of factors, but very few of them recognise the importance of the evaluation of these technologies before adoption (Ren 2019; Sadoughi et al. 2019). Similarly, studies that link poor uptake of cloud services to evaluation make little attempt to explain how SMEs can evaluate Cloud BI and the tools available to attain such a difficult feat.

### **2.6.1. Understanding security evaluation in cloud business intelligence**

The adoption of Cloud BI and the migration of data and application to the cloud is a critical decision that requires SME decision-makers to have insights into various operational and security functionalities important to the usability and security of cloud services (Cooper 2017; Wise 2016). Literature shows that Cloud BI are more susceptible to security flaws, cybersecurity threats, and risks in the cloud environment than traditional IS applications and network infrastructure (Fernandes et al. 2014; Agostino et al. 2013). This illustrates that the evaluation process is important in ensuring that appropriate decisions are made based on the expectations of SMEs about the effectiveness of security controls and operational functionalities of Cloud BI.

In light of this, the purpose of the evaluation process is guiding, planning, and verifying whether CSPs properly implement the correct security procedures and that appropriate operational controls are in place in the Cloud BI (Columbus 2020; Cloud Standards Customer 2017; Ramachandran & Chang 2016; Akinbi 2015). Ultimately, decision-makers need to understand basic security evaluation for them to embark on the selection of Cloud BI. In this context, the purpose of the evaluation process would be to provide decision-makers with an opportunity to systematically collect and analyse data and then use the information to judge the worthiness and effectiveness of Cloud BI in attaining planned objectives (Mussa et al. 2016). The assumption is that a proper evaluation can provide useful feedback which can be used to justify the adoption. This clearly

illustrates that decision-makers require up-to-date information about Cloud BI to make correct decisions on the course of action to take.

Traditionally, IT systems, applications and products are evaluated to establish the quality of the product during the development life cycle and the product evaluation is intended to establish how best the supplier's promises about a product meet the customer's needs (Cooper 2017; Wise 2016). In SMEs, product evaluation is preferred because it enables decision-makers to check whether the quality, user satisfaction, functionalities and operational environment's security meet business needs and security expectations (Al-Yaseen, Eldabi, Lees & Paul 2006; Hallikainen & Chen 2005). This means that Cloud BI need to be subjected to a thorough security evaluation, thus a broader evaluation than only considering security vulnerabilities and cybersecurity threats as suggested in several studies (Subramanian & Jeyaraj 2018; Opara-Martins et al. 2016).

Two commonly used evaluation techniques with IS systems and applications are *prior-operational-use evaluation (POUE)* and *operational-use evaluation (OUE)* (Mussa et al. 2016; Al-Yaseen 2012). Each type of evaluation is conducted to support a certain decision process for each stage of the IT system or application life cycle. POUE or strategic pre-implementation evaluation is performed to predict estimated costs, benefits and return on investment to support and justify decisions for investing in a given IT system (Al-Yaseen et al. 2010). The OUE is conducted to establish the actual positive or negative impact of the new IT system to gain knowledge on how the system performs to accomplish the objectives it has been designed for (Al-Yaseen 2012; Al-Yaseen et al. 2010). The POUE can be adapted for the security evaluation of Cloud BI by SMEs to provide essential information about Cloud BI that can be used to make decisions on whether to adopt the technology. By using POUE, an enterprise embarks on a feasibility study to assess security vulnerabilities, threats and risks likely to hinder the use of the technology in question when adopted.

Although there are strong recommendations from various studies for SMEs to evaluate cloud services, presently there is a lack of common understanding of how SMEs should do this (Wise 2016; Agostino et al. 2013). This lack of a common standpoint is indicative of different perspectives among various authors on what aspects of Cloud BI should be evaluated.

Furthermore, Dabrowska and Cornford (2001) argue that the IS evaluation process is complex as shown by the lack of an agreement on ideal methods to evaluate or to improve the evaluation process. The authors emphasise that the evaluation process in IS will remain a critical activity, which needs to be performed thoroughly during the life span of each system. Despite the challenges that are likely to be faced, decision-makers should evaluate Cloud BI before adoption to avoid business failures due to security and financial risks.

### **2.6.2. Initiatives in cloud business intelligence evaluation before adoption**

With the growing emphasis on the need for SMEs to adopt and use cloud services, many piecemeal solutions to the evaluation processes are advanced to offset challenges posed by conventional techniques, such as vulnerability scanning and testing used by LBEs with functional finance and IT security personnel (Pantić & Babar 2019; Kazim & Zhu 2015). Consequently, security evaluation initiatives for Cloud BI put forward by several studies have remained similar to those of traditional IS and include the application of vulnerability assessment and penetration testing (VAPT), standards, frameworks, checklists, policies and guidelines (Ramachandran & Chang 2016; Chou 2013; Winkler 2011). The presence of many evaluation initiatives with diverse standards shows the complex nature of the challenges that cloud services adopters could face in their effort to evaluate the cloud services when selecting the appropriate evaluation tools (Eldabi, Paul & Sbeih 2008; Hallikainen & Chen 2005).

#### **i. Vulnerability Assessment and Pen Tests results**

Current evaluation practices rely mainly on vulnerability assessments and penetration testing (VAPT) results, the two popular conventional methods for evaluating information system vulnerabilities (Deepa & Thilagam 2016; Gupta & Kaur 2013). There is a plethora of literature discussing the benefits and limitations of VAPT methods related to traditional information systems (Durg & Podder 2020; Ramachandran & Chang 2016; Chang, Kuob, et al. 2015). While vulnerability assessment is conducted to test the security position of the IS internally and externally, a penetration test is conducted to gather evidence on the actual existence of vulnerabilities and possible threats in the network (Deepa & Thilagam 2016; Gupta & Kaur 2013). CSPs use penetration tests to assess services provided by identifying existing security vulnerabilities, missing patches, and misconfigured firewalls (Bacudio, Yuan, Chu & Jones 2011).

Penetration testing is complex and requires expertise way beyond SMEs' financial means and is beyond the scope of this study. However, decision-makers can request the results of these tests from CSPs and then analyse them for adoption purposes (Bacudio et al. 2011). This can pose a challenge to the decision-makers as they might not get the results from the CSPs or fail to interpret the results altogether.

The possibility of SMEs performing vulnerability assessments using vulnerability scanners is slim considering the conditions under which these are performed, and the technical know-how required. Vulnerability assessment requires SMEs to utilise scanners to identify and analyse different security weaknesses in enterprise information systems, devices and software owned by CSPs to predict the effectiveness of countermeasures (Kupsch, Miller, Heymann & Cesar 2010). Vulnerability assessment can be manual or automated (Tiwari & Mishra 2012; Bacudio et al. 2011). Automated assessments are preferred over manual ones because they are simple to perform (Deepa & Thilagam 2016; Khorshed, Ali & Wasimi 2012). However, these evaluation methods may not be feasible before the adoption of applications because CSPs can be reluctant to allow SMEs to do so (Al-Yaseen 2012).

ii. Security standards and frameworks, policies, guidelines, and checklists

Security policies, standards, and guidelines have been used in security evaluation in IT systems, including Cloud BI (Ajibade 2018; Choi & Lee 2015). Although SMEs are encouraged to use these tools, they might not be able to interpret the policies and the standards needed to evaluate Cloud BI.

*Security standards and frameworks:* These are interrelated security evaluation tools whose usefulness and acceptance are widely documented (Granneman 2019; Cloud Standards Customer Council 2016; Gleeson & Walden 2014). *Security standards* provide industry or government-approved specifications against which the qualities of an IS can be measured (Mirai Security 2019; Perkins 2016). These can be standardised process documents developed to support specific policies or requirements (Rezaei, Chiew & Lee 2013; Rostek et al. 2012). The use of standards is a unanimously accepted norm because it provides the basis for matching a selected security system



with a given frame of reference recognised nationally or internationally (Information Security Forum 2016; Tofan 2011).

On the other hand, *security frameworks* are standards for best practices used for certification and usually define specific policies, controls, checklists, and procedures (Granneman 2019; Cloud Standards Customer Council 2016). This tells us that both standards and frameworks are needed to guarantee the desired features of products and services such as quality, safety, reliability and efficiency in a cost-effective manner (Perkins 2016; Tofan 2011). Many publicised standards and frameworks include: (1) the Control Objectives for Information and Related Technologies (COBIT); 2) the International Standards Organisation (ISO) 27000 series; 3) National Institute of Standards and Technology (NIST); 4) Information Security Risk Management Framework (ISRMF- ISO 31000 ); 5) The Healthcare Insurance Portability and Accountability Act (HIPAA); and 6) the Payment Card Industry's Data Security Standard (PCI DSS) (Indriasari et al. 2018; Rupra et al. 2018; Broughton 2017; Iqbal et al. 2016; Tiwari 2010). Literature touts these tools as being more suitable for large IT systems, particularly those found in LBEs managed by security specialists but rarely found in SMEs (Cloud Standards Customer Council 2016; Opara-Martins et al. 2016; Ibrahim & Musah 2015).

The *COBIT* is portrayed as a complex framework for IT governance used in identifying and mitigating risk in the financial industry, but its lack of practical use by itself makes it unsuitable for use by SMEs (Rupra et al. 2018; Wild 2018). The COBIT requires a detailed standard such as ISO 27001 for successful implementation (Cloud Standards Customer Council 2016; Information Security Forum 2016). The *ISO 27001* Cybersecurity framework bundles together several international standards to provide requirements for managing information security management systems (Choi & Lee 2015). The ISO 27001 recommends risk-based procedures by which businesses and enterprises would set methods for detecting security threats that impact their information systems (Gleeson & Walden 2014; Huang & Nicol 2013). According to Werff et al. (2019), the ISO 27001 is mature, comprehensive and broad, and allegedly useable in IT information systems of enterprises in different economic activities. Multiple versions of the ISO 27001 raise concerns to SMEs who may have challenges interpreting several technical issues being addressed by this framework.

Furthermore, the *NIST* cybersecurity framework is regarded as a collection of several information security standards and best practices for different types of enterprises (Ramachandran & Chang 2016; Agostino et al. 2013; Subashini & Kavitha 2011). The NIST is viewed as an established and comprehensive framework most appropriate for LBEs and can be adapted to SMEs (Rupra et al. 2018; Wild 2018; Mogull et al. 2017). The problem with the NIST is that it is vast and complex for SMEs with small IT infrastructure and a lack of technical ability to implement it (Mirai Security 2019; Mashandudze & Dwolatzky 2015).

The *ISRMF* is a collection of processes and practices that enterprises using IT information systems can use in identifying, evaluating, and treating risks within an enterprise's key information asset (Broughton 2017; Information Security Forum 2016; Tiwari 2010). By using the *ISRMF*, security managers are expected to identify, with great accuracy, the most vulnerable assets in the enterprise and be able to prevent threats from exploiting the vulnerabilities (Rupra et al. 2018; Fernandes et al. 2014; Khorshed et al. 2012). The *ISRMF* is ideal for traditional IT systems where enterprises have more control than in cloud services.

The *HIPAA* provides for the protection of medical information that enterprises should exercise (Mirai Security 2019; Mogull et al. 2017). *PCI DSS* stipulates a set of security standards to compel enterprises to process, store, or transmit credit card information in a secure environment (Information Security Forum 2016). SMEs in these economic sectors are expected to be acquainted with these standards to check if the Cloud BI to be adopted matches the enterprise security requirements. Without technical assistance from IT specialists, SMEs may face challenges in using conventional frameworks when evaluating new IT solutions.

Conventional frameworks are appropriate for use by enterprises already using IT systems and have specialists to undertake activities about security. However, they may not be ideal for use as adoption frameworks in SMEs, particularly in small towns where the use of cloud services is not yet a norm. (Mirai Security 2019; Calumpang & Dilan 2016). Furthermore, these frameworks are more appropriate for OUE than POUE, where an enterprise has already adopted the application. This means that SMEs are generally without suitable frameworks to cater to their business needs when adopting Cloud BI.

**Policies:** Studies and reports in IS show that security policies are important because they define an enterprise's requirements or rules for security, by specifying constraints that individuals and groups must operate under (Shimamoto 2015; Winkler 2011). For example, Vacca (2017) posits that CSPs are compelled to show their clients documented policies and procedures they use when requested. This development can make it possible for SMEs to obtain policies from CSPs for scrutiny purposes to ascertain transparency. Under such situations, clients can use policies to evaluate cloud services from a technological perspective (Choi & Lee 2015; Hashizume et al. 2013; Winkler 2011). It is assumed that upon receipt of the policies from CSPs, SMEs will be able to get the information required to evaluate Cloud BI. However, this can be a difficult task to achieve because of communication barriers with CSPs.

**Guidelines** are recommendations, best practices or support documents and processes that help with the interpretation and implementation of policies and requirements (Ajibade 2018; Perkins 2016; Elena & Johnson 2015b; DeCarlo 2011). The ISO 27001 and the NIST frameworks provide guidelines for addressing essential issues in cloud security and privacy, including architecture, identity and access management, trust, software isolation, data protection, compliance, availability and incident response (Mirai Security 2019; Gleeson & Walden 2014). The main problem with most of the frameworks is that they can only be implemented by security specialists, the personnel not found in SMEs.

Notably, the Cloud Standards Customer Council (2017) proposes guidelines for evaluating and managing security in applications in cloud environments by enterprises already using cloud services or those intending to adopt them. The Cloud Standards Customer Council (2017) emphasises the evaluation of CSPs for good governance and risk complaint processes which safeguard enterprises' operational and business needs. The major limitation of the guidelines is that client enterprises have to physically access the CSPs to evaluate the physical infrastructure at the data centres. This is highly impossible, considering that CSPs can have data centres distributed in different geographical areas.

**Checklists** are widely reported evaluation tools used by several organisations (Rupra et al. 2018; Cloud Security Alliance 2016; Gartner 2016; Vohradsky 2012). A study by (Shuaibu, Norwawi,

Selamat and Al-Alwani (2015) reports many advantages of using checklists in cloud security evaluation. Unlike automated VAPTs, evaluation checklists can easily be used by potential cloud clients to compare cloud services from different CSPs in terms of security and other criteria (Elena & Johnson 2015b; ENISA 2015; Carcary et al. 2014). Winkler (2011) suggests a security evaluation checklist that can be implemented by cloud owners and prospective cloud clients such as SMEs, which consists of four key components, namely, foundational security, defence-in-depth, operational security and business considerations. Each of the components has criteria that the evaluator uses in the assessment. According to Winkler (2011), a cloud security evaluation checklist acts as a means to provide reliable information to verify the security of cloud services while obtaining assurance from a CSP about their security. However, the shortcoming of Winkler's checklist is that its structure makes it labour intensive to complete when evaluating CSPs.

eSentire Managed Security Services (2012) developed a comprehensive checklist for evaluating CSPs based on the risk management standards and guidelines that were crafted by ENISA in 2009. The eSentire Managed Security Services (2012) alleges that the cloud checklist has been well-received by financial institutions in exploring the use of cloud services. By completing the checklist, cloud service adopters were able to determine threats, vulnerabilities and risks within the targeted cloud services (Cloud Standards Customer 2017; Cloud Standards Customer Council 2016). What is worth noting, is that the eSentire emphasises CSPs predominantly and pays little attention to other important aspects of cloud security.

## **2.7. Security evaluation challenges for cloud business intelligence**

Existing studies on cloud services adoption focus on the benefits and risks that influence the uptake of the technology and very few try to understand the challenges faced by SMEs when evaluating these applications (Salim et al. 2015). With an increase in the acceptance of Cloud BI among SMEs in South Africa, one would expect a surge in the uptake of the technology. According to Agostino, Soilen and Gerritsen (2013), the presence of several Cloud BI from different CSPs has different security issues; which pose selection challenges to decision-makers and this perpetuates the marginalisation of SMEs. Vacca (2017) purports that the evaluation of Cloud BI obliges enterprises to assess several aspects of the cloud, contrary to traditional BI, in which technical and procedural aspects are assessed. However, the results on the ground show a different scenario

because the evaluation is regarded as the responsibility of the enterprises involved (Hurtaud & de la Vaissière 2017; Sherman 2015). It is important to note that several studies assume that SMEs already have sufficient technical skills and knowledge to conduct evaluations on their own (Boonsiritomachai et al. 2014). Documented challenges to security evaluation among SMEs are associated with knowledge and skills in security evaluation; the complexity of evaluation tools available; and the availability of relevant information from CSPs about the Cloud BI being offered.

### **2.7.1. Knowledge of security evaluation in cloud business intelligence**

Knowledge about the impact of cloud services on business operations is important for SMEs to consider when selecting the appropriate cloud services (Flack 2016; Patel & Connolly 2007). This requires decision-makers to assess and evaluate possible Cloud BI from a cluster available. Besides knowing Cloud BI and how they work, decision-makers should be able to determine how secure the applications are, which entails basic knowledge in the security evaluation of application requirements (Igli & Solange 2019; Sentilles, Papatheocharous & Ciccozzi 2018; Calumpang & Dilan 2016). The importance of knowledge in evaluating technologies is highlighted by the DoIT, which emphasises the relative advantage, compatibility, complexity, observability, and trialability of a technology (Beever 2018; Fry et al. 2018; Meijer et al. 2015).

A study by Santos-olmo *et al.* (2016) reports that SME decision-makers do not have the appropriate insights into the importance of information security in business, and therefore, do not see any need to evaluate the IT applications they adopt and use. Oza, Karppinen and Savola (2010) assert that decision-makers who lack security knowledge tend to overlook assessing security threats, provided that their information systems availability is uninterrupted. Similarly, Lacey and James (2010) reported that SME decision-makers tended to reduce their obligations and contribution to security matters in enterprise information systems because they did not view security as their responsibility. This shows that decision-makers with little security know-how would regard expenses in securing IT information systems as unnecessary and avoidable overhead. Limited knowledge about security evaluation can be a major challenge for decision-makers when assessing Cloud BI in order to select the most appropriate application (Hussein & Khalid 2016).

### **2.7.2. The complexity of industry security evaluation framework and standards**

SaaS has transformed how enterprises acquire IT solutions and this compels SME decision-makers to be involved in the evaluation process; if they are to make correct decisions about which applications to adopt (Elmalah & Nasr 2019; Phneah 2013; Sheikh 2011). However, decision-makers may face challenges in using existing evaluation tools which have been proven to be complicated for non-IT specialists (Matikiti, Mpinganjira & Roberts-Lombard 2018; Malak 2016). It cannot be overemphasised that most of the existing security evaluation tools and methodologies are ideal for large IT systems, particularly in LBEs where they are managed by IT specialists (Mirai Security 2019; Boonsiritomachai et al. 2014). Complexities in evaluation tools and methodologies can discourage decision-makers from performing evaluations, thereby compelling the enterprises to adopt compromised Cloud BI or to continue to use old IT systems.

Mirai Security Inc (2019) observes that traditional security frameworks and standards are vast and difficult to use by SMEs. Several non-conventional frameworks are specific to certain aspects of IT solutions and the types of business problems they are designed to solve (Cloud Standards Customer 2017; Alliance 2015). Cloud BI can be beneficial to SMEs, but there is no guarantee of this because of evaluation challenges. The lack of standardisation in Cloud BI provided by various CSPs means that decision-makers will have to craft strategies to evaluate cloud technologies (Akinbi 2015), a feat that may prove difficult to achieve.

### **2.7.3. Lack of information on cloud business intelligence from service providers**

The importance of information in decision-making is emphasised by DoIT (Fry et al. 2018; Meijer et al. 2015), TPB, and MSAM adoption theories (Lamb 2016; Salim et al. 2014, 2015; Ettlíe & Penner-Hahn 1994). Hurtaud and de la Vaissière (2017) argue that security concerns in Cloud BI are due to the fear that enterprise data stored in CSPs data centres can be compromised and have negative consequences for enterprise information systems. This compels decision-makers to seek more information about CSPs and the security of the services being offered (Rizvi et al. 2018; Elena & Johnson 2015b; Rivastava & Kumar 2015). Literature suggests sources from which information about a CSP can be obtained, namely: the respective CSP website and direct contacts, friends, discussion forums, and security publication sites (Salum et al. 2016; ENISA 2015; Salim et al. 2015). However, only part of the information from well-established CSPs can be accessed

and used by decision-makers. Furthermore, some websites' information can be out-dated or no longer relevant to the needs of the enterprise. Unlike security review publications, which give current information about security breaches and vulnerabilities in Cloud technologies, CSPs might not be prepared to do so and do not divulge this information due to fear of losing business from potential customers (Khan & Al-Yasiri 2015; Khanagha, Volberda, Sidhu & Oshri 2013). SME decision-makers who are used to conventional ways of obtaining information can face challenges in finding relevant information about CSPs from different sources.

## **2.8. Security evaluation frameworks for cloud business intelligence**

The mainstream security frameworks in use today, have been designed to assess security in specific areas of the cloud computing industry (Elmalah & Nasr 2019; Pantić & Babar 2019; Rizvi et al. 2018). Very few security frameworks for evaluating Cloud BI, suitable for SMEs, exist (Mirai Security 2019; Olszak 2014). Most of the security frameworks have been criticised for being vast, complicated, broad in scope, specific to a certain industry, incompatible with systems used by SMEs, and demanding IT expertise for implementation (Durg & Podder 2020; Mirai Security 2019; Rupra et al. 2018). This means that such security frameworks may present challenges when used by non-IT specialists in evaluating Cloud BI (Durg & Podder 2020; Olszak 2014). For example, Rizvi *et al.* (2018) present a security evaluation framework for auditing CSPs consisting of both conceptual and quantitative models. The framework depends on quantitative data from CSPs, which SMEs may find difficult to find. The quantitative nature of the framework makes it more difficult for SMEs to use without guidelines to assist users during the evaluation process. However, the framework remains important in theory and practice because it gives insights into challenges that enterprises face when they embark on evaluating cloud services.

Rupra, Karie and Rabah (2019) propose a framework for assessing security in a SaaS for use by SMEs. The framework provides key areas to be evaluated in SaaS but focuses more on technical issues and fails to explain how SMEs should use the framework. Therefore, the framework is more suitable for enterprises already utilising SaaS (Rupra et al. 2018). Additionally, a study by Rostek, Wisniewski and Kucharska (2012) proposes a practical cloud computing security framework for Cloud BI adoption by SMEs. The framework indicates specific areas that SMEs would consider

when evaluating Cloud BI, but due to its technical nature, it is too complicated for SME decision-makers.

Lastly, the European Union Agency for Network and Information Security, (2015) developed a security framework, Plan-Do-Check-Act (PDCA), to demonstrate information security management systems in government public clouds. The PDCA provides guidelines on how government institutions can deploy and use various cloud service delivery models. The framework requires experts to perform the required evaluation on behalf of the enterprises. In its current form, the PDCA cannot be of much use to SMEs who lack security evaluation expertise and financial resources to hire experts. The framework assumes that enterprises should have already adopted cloud services, which might not be the case with most SMEs in small South African towns. The PDCA is a labour-intensive framework, and this may deter SMEs from using it.

The importance of a security evaluation framework lies in its ability to assist enterprises to implement specific standards, policies, controls, checklists, and procedures to assess and measure CSPs' conformance (Moraetes 2018; Cloud Standards Customer Council 2016; Khan 2012). According to Chang, Kuob and Ramachandran (2015), a security evaluation framework can aid decision-makers to assess and evaluate vulnerabilities, threats, and risks and then recommend the best practices that encourage SMEs to use proper procedures in the successful adoption of Cloud BI. It is a common practice to customise an existing framework and use it to solve identified information security problems whenever a need arises (Calumpang & Dilan 2016; Chang, Kuob, et al. 2015). Some studies emphasise the designing of suitable frameworks if there is no existing one, but the process is laborious (Hussain et al. 2018; European Union Agency for Network and Information Security 2015). Customising an existing framework produces results quickly, but retains the flaws of the original framework that might affect the evaluation results (Akinbi 2015).

Although different authors seem to agree on the importance of security evaluation of cloud services before adoption, they offer divergent views on what constitutes an evaluation framework (Hurtaud & de la Vaissière 2017; Senarathna et al. 2016; Kasem & Hassanein 2014). This has increased frameworks emphasising different aspects. Some studies regard the evaluation of vulnerabilities, threats, and risks in cloud technologies as the most important aspect to consider but disregard the financial characteristics of the adopter (Mirai Security 2019; Ren 2019; Lacey & James 2010).



Other studies emphasise the economic benefits and risks but tend to ignore technological risks (Tutunea & Rus 2014; Guarda, Santos, Pinto, Augusto & Silva 2013). A few studies emphasise the evaluation of security in the deployment models as well as the CSPs (Rupra et al. 2018; Devesh et al. 2017; Ngeru & Bardhan 2015; Romes 2015). It is against this background that an integrated security evaluation framework for Cloud BI, tailored for SMEs in small South African towns, would be used.

### **2.8.1. Data security and application security**

Studies on cloud service adoption and use focus much on data and application security (Fernandes et al. 2014; Rezaei et al. 2013). These studies suggest that enterprise data and application security need to be taken seriously during the evaluation process. According to Juan-Verdejo and Baars (2013), SMEs intending to adopt Cloud BI or migrate data and applications to the cloud should analyse and assess all business needs and data management requirements to make correct decisions on the security requirements of enterprise data. The Cloud Security Alliance (2015) suggests that enterprises should undertake a proper risk identification and evaluation before the adoption of any cloud services. The risk assessment component involves identifying data and applications to be migrated to the cloud and determining the security requirements of the identified data and applications before deployment in the cloud. This implies that decision-makers will have to implement the ISRMF and ISO 270001 frameworks in the risk assessment process to determine the importance of data and applications to the enterprise in terms of CIA requirements for assets, changes and risks of deployment in the cloud (Hurtaud & de la Vaissière 2017).

### **2.8.2. Business benefits and risks of adopting the cloud business intelligence**

When adopting Cloud BI, enterprises need to safeguard business benefits against risks (Agostino et al. 2013; Thompson & van der Walt 2010). As a precautionary measure, Willcocks (1992) suggests that enterprises should include formal and informal evaluations as a means to assess business benefits, costs, risk, and the value of an IT system to the enterprise. This draws from the DoIT's relative advantage, observability, and trialability of the technology (Devesh et al. 2017; Salim et al. 2014; Alshamaila et al. 2013). A security evaluation framework should enable decision-makers to assess intangible and tangible benefits and risks of adopting and using Cloud BI before the adoption, as recommended by Wen and Sylla (1999).

Care is needed to prevent enterprises from focusing the evaluation on business aspects while ignoring influential technological and environmental aspects to the adoption of Cloud BI (Sadoughi et al. 2019; Hallikainen & Chen 2005). However, the focus of the evaluation can vary with the evaluator and its purpose (Hallikainen & Chen 2005) or business interests emanating from different challenges and expectations, such as improving service, cutting costs and gaining competitive advantage (Farbey, Land & Target 1992). Literature shows that the enterprises tend to overlook the evaluation of risks of additional costs; disruption of business operations and customers; loss of customers of competitors; and exposure when a system malfunctions (Ereth & Dahl 2013; Willcocks 1992). This indicates the importance of the ISRMF in the security evaluation framework to enable decision-makers to assess benefits and risks at the onset of the evaluation. This highlights the need to integrate business benefits and risks assessments with data and application security during the evaluation of Cloud BI before adoption.

### **2.8.3. Cloud deployment models**

Security benefits and risks depend on the cloud deployment models used to provision cloud service delivery services, therefore, this requires much consideration during the evaluation process (Vacca 2017; Shimamoto 2015; Cloud Security White Paper 2011). Some authors are of the view that SMEs should evaluate and select cloud deployment models provided by CSPs, based on performance requirements; existing interdependencies; network costs; security; and privacy essentials (Koparkar & Mackrell 2015; Sadler, Lee, Lim & Fullerton 2010). SMEs are inclined to adopt Cloud BI deployed in public clouds, which have both accessibility and cost benefits. However, public clouds have the lowest security assurance for data-in-storage and data-in-processing (Fernandes et al. 2014; Hooda 2014). Consequently, SMEs interested in Cloud BI from private and hybrid clouds may have fewer security considerations than those interested in Cloud BI available in public and community models (Yauri & Abah 2016; Ngeru & Bardhan 2015). By using the ISRMF and the NIST cybersecurity frameworks, decision-makers can evaluate all four cloud deployment models to select the most appropriate one that matches their business needs. However, if decision-makers lack security know-how it will be difficult for them to use the evaluation tools.

#### **2.8.4. Cloud service providers**

The literature reviewed in previous sections has illustrated that CSPs play an important role in the uptake and use of cloud services and this has a bearing on the security framework for evaluating Cloud BI (Rupra et al. 2018; Ereth & Dahl 2013). For the SaaS Cloud BI in the public and community models, the CSP provides infrastructure, software, and security while client enterprises configure their systems and procedural security (Santos-olmo et al. 2016; Winkler 2011). This makes CSPs an important aspect of the evaluation framework in which SMEs need assistance when evaluating Cloud BI. Hurtaud and de la Vaissière (2017), suggest that when SMEs evaluate potential CSPs, they should focus on the degree of control the enterprise will have in implementing risk mitigation and other security requirements in each cloud deployment model.

The Cloud Security White Paper (2011) emphasises that enterprises should assess the physical infrastructure in CSPs' data centres; the applications hosted by CSPs that enterprises use for data processing and management; and the standards, policies and procedures used to provide and maintain security in the cloud. This is reiterated by Shimamoto (2015) who argues that enterprises must have insights into IT infrastructure security, data security, security standards, and processes concerning cloud applications to be adopted. However, the complexity in cloud architecture can make it difficult for CSPs to divulge the physical data location to the SMEs, which in turn makes the evaluation of the physical security of data centres practically impossible (Sherman 2015). During the evaluation process, decision-makers are encouraged to question CSPs about data security at the data centres (Devesh et al. 2017; Saunders, Lewis & Thornhill 2012). Jakimoski (2016) emphasises the importance that SME decision-makers must only select Cloud BI after evaluating security weaknesses, threats, and risks, controls in place, and data storage. Literature emphasises the thorough assessment of CSAs and SLAs offered by different CSPs based on the enterprise business requirements and security policies. This shows that security policies are important parts of a security evaluation framework that can assist SMEs to evaluate CSPs.

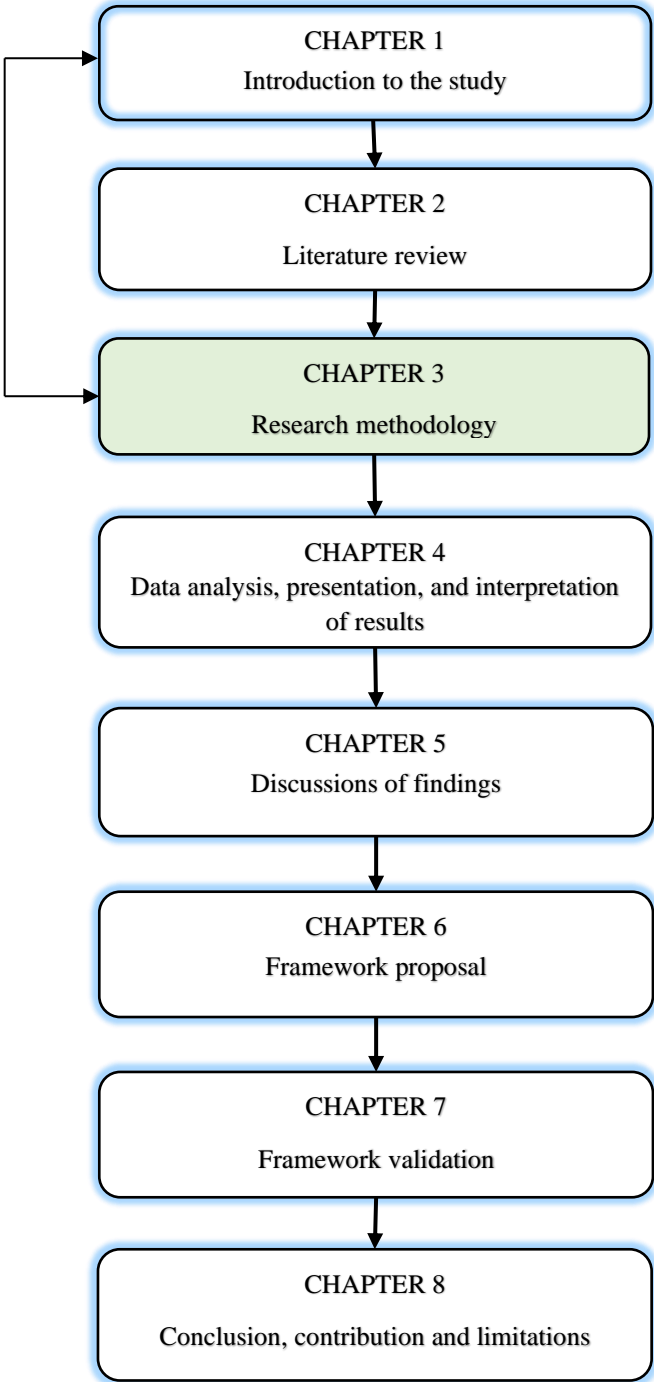
#### **2.9. Conclusion**

The chapter presents the literature on Cloud BI deployment and business benefits to SMEs. Factors influencing the adoption of Cloud BI have been explored using theories of technology adoption namely, the TPB, TAM, DoIT and MSAM. The major influential factors have been identified as

benefits, security risks in the applications, and cloud environment characteristics of enterprises and CSPs' trusts. The literature shows that the security evaluation tools currently being used are too complex for SME decision-makers with limited security knowledge in IT systems. The literature identified a host of possible challenges likely to affect security evaluation in Cloud BI by SMEs without access to IT security specialists. There is evidence from the literature that no consensus exists on what should be evaluated and how the evaluation process should proceed, placing the responsibility into the hands of decision-makers.

The literature review presented supports this view and further argues that the absence of a user-friendly security evaluation framework for use by SMEs, exacerbates the adoption challenges. The next chapter presents a detailed research methodology and design used.

**CHAPTER 3 RESEARCH METHODOLOGY**



### **3.1. Introduction**

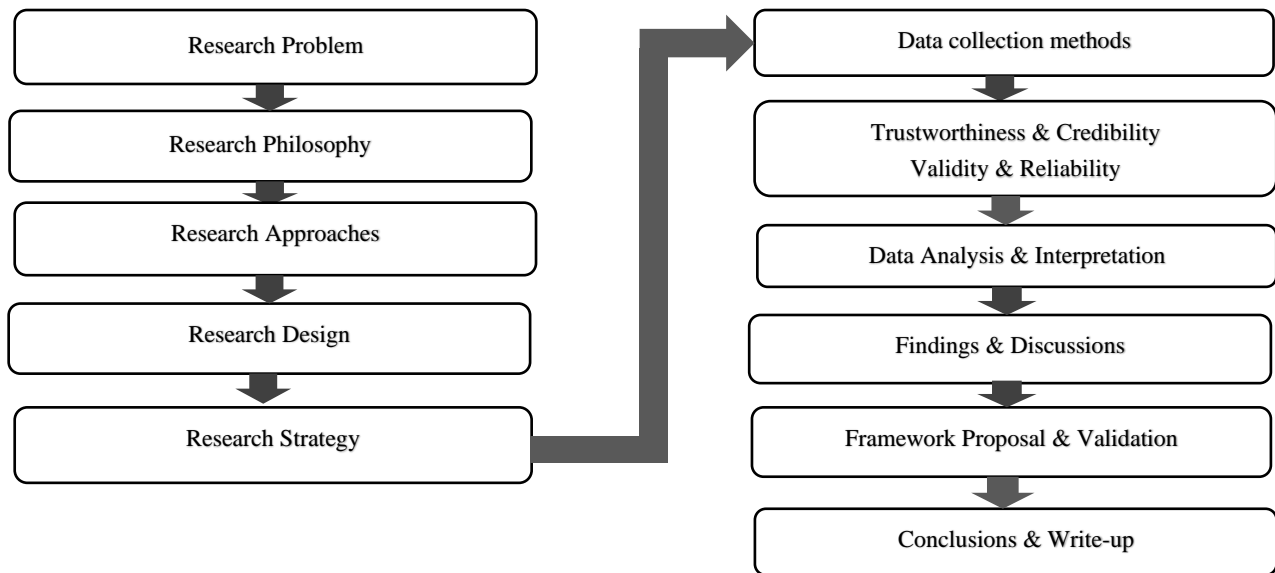
The purpose of this chapter is to describe and justify the research methodology followed in this research study. This chapter is organised as follows: introduction, research methodology, research philosophy, research approaches, research designs, research strategy, population and sampling strategy, data generation and analysis techniques, validity, reliability and trustworthiness, ethical consideration, and conclusion.

### **3.2. Research methodology and design**

Research methodology refers to the overall systematic approach to the design process of doing research, starting from theoretical underpinnings to the collection and analysis of data (Creswell & Creswell 2018; Scott 2016). According to Wu (2012), methodology refers to matters regarding the structure and design of the research study. The research methodology used in this study was selected based on the research problem being solved and the nature of the data needed to answer the research questions (Zefeiti & Mohamad 2015; Nachmias & Nachmias 2008). The research methodology used guided the overall approach and perspectives adopted to the research process as a whole. According to Creswell and Creswell (2018), a research methodology is important in assisting the researcher to maximise the credibility of the results and findings of the research study. Furthermore, a researcher needs to understand the research methodology to identify and decide which research design works most efficiently when investigating a given problem (Creswell & Creswell 2018; Paulinus & David 2013).

Both qualitative and quantitative data about the experiences and feelings of decision-makers were required to answer the research question and to propose a suitable security framework for Cloud BI, which SME decision-makers, who are non-IT specialists, can use.

The research process for this study was adapted from the Research Onion Model (ROM) by Saunders et al. (2012), which specifies a simple research methodology. The ROM was selected due to its thoroughness, and it is easy to understand and implement the solution to the research problem being addressed. Figure 3.1 shows the sequence of steps in the research methodology and design used in this study.



**Figure 3.1: Research process**  
Adapted from Research Onion Model Saunders et al. (2012)

A detailed discussion of each step is presented in subsequent sub-sections of this chapter.

### 3.2.1. Research philosophy

After presenting the research problem in Chapter 1, and the literature review in Chapter 2, there was a need to elucidate the philosophical perspective used to understand and solve the problem pursued by this study. The realistic worldview of the researcher and the research philosophy or paradigm, which helped to choose the strategy, design, and methods, needed to solve the problem influenced the process of problem understanding (Creswell & Creswell 2018; Gray 2013). Research philosophy is defined as a set of assumptions, concepts, values, and practices that constitute a way of viewing reality (Farjoun, Ansell & Boin 2015; Morgan 2014a). Research philosophy is needed to guide a researcher in the process of knowledge development and the nature of the knowledge to be developed (Mkansi & Acheampong, 2012). Saunders et al. (2012) and Mkansi and Acheampong (2012) provide three justifications for researchers to understand research philosophies in connection with research methodology in their studies.

Firstly, an understanding of the underlying research philosophy guides the refinement and clarification of the chosen research methods employed to gather the necessary evidence towards

addressing the research questions (Pathirage, Amaratunga & Haigh 2016; Mkansi & Acheampong 2012). Secondly, the researcher's knowledge of research philosophy, assisted by different types of methodologies, helped in the selection of the appropriate literature (Pathirage et al. 2016; UK Essays 2015; Saunders et al. 2012). Once the research philosophy was identified, the researcher conducted a literature review based on studies that utilised the same paradigms. Thirdly, by understanding the merits and benefits of each research philosophy, the researcher became more creative and exploratory in selecting research methods (Pathirage et al. 2016; Zefeiti & Mohamad 2015; Mkansi & Acheampong 2012). The Research Onion Model clearly distinguishes several research philosophies that can be utilised in various research studies, but categorically emphasises positivism, interpretivism, realism, and pragmatism. Only three research philosophies that have a bearing on this study were presented, namely positivism, interpretivism and pragmatism.

#### **i. Positivism**

Positivism is a widely used philosophical approach based on objectivism in which researchers are obliged to provide an objective point of view when evaluating phenomena in the social world (Johnson, Yasugi, Sugino, Pranata & Shen 2018; Venkatesh, Brown & Bala 2013). A researcher utilising positivism is always expected to collect information and data from a large sample rather than paying attention to details of research (UK Essays 2015; Mkansi & Acheampong 2012). Positivism stipulates that the researcher's own beliefs and perceptions of the phenomenon should not affect the findings of a research study (Rahman 2017; Cameron 2015). The proponents of the positivist paradigm purport that true knowledge is solely based on the experience of senses which can be acquired through observation and experiment, and therefore, emphasise that the best way of exploring social reality is to understand human behaviour through observation and reason (Timans, Wouters & Heilbron 2019; Edirisingha 2012; Goldkuhl 2008). Positivist ontology assumes that the reality should be objectively given and measured by the utilisation of strategies and properties free from the influence of the researcher and the research tools applied in the research (Johnson et al. 2018; Myers & Avison 2011). This implies that positivists regard knowledge as objective and quantifiable (Edirisingha 2012; Sekaran & Bougie 2012). According to Henning, Van Rensburg and Smit (2006), positivism is mainly concerned with finding the truth and presenting it by empirical means.



Positivism is a viable philosophical approach if the research study deals with a stable and fixed reality for the researcher to be able to justify the adoption of an objectivist perspective (Alharahsheh & Pius 2020; Mkansi & Acheampong 2012; Henning et al. 2006). In this regard, the researcher's epistemological stance is completely detached from the beliefs and perceptions of the respondents or research subjects (Bonache 2021; Chandra, Seidel & Gregor 2015; Teddlie & Tashakkori 2009). The adoption of Cloud BI by SMEs can be influenced by multiple factors that cannot be determined completely from a positivist approach. Mitigating factors are dynamic and may require subjective judgement by the researcher and those involved in the study. Positivism alone cannot be used to research decision-makers' understanding of Cloud BI or their disposition to security threats and other social issues because of the different circumstances in which these technologies are used. The environment in which Cloud BI is utilised is unstable due to differences in technologies used and rapid changes which make it difficult to implement positivist philosophies on their own.

## **ii. Interpretivism**

Contrary to positivism, studies using interpretivism seek to understand the phenomenon by exploring and explaining participants' beliefs, insights, textual and verbal information, communal ideals and behaviour, and their connotations in changing social contexts (Alharahsheh & Pius 2020; Zalaghi & Khazaei 2016; Saunders et al. 2012). The adoption of Cloud BI is a social phenomenon influenced by several factors, such as vulnerabilities in the technology, cyber threats, and contextual factors which are beyond the control of clients and CSPs. This requires the researcher to understand the experiences, feelings, beliefs, perceptions, and knowledge of decision-makers from an interpretive perspective.

Leitch, Hill and Harrison (2010) posit that interpretivism is a lifeworld-based ontology that views observation as being both theory and value-laden methods. Therefore, the researcher's experience about the phenomenon being researched may influence how the truth is established. The epistemological stance of interpretivism is that knowledge is a result of social construction by human actors (Alharahsheh & Pius 2020; Paulinus & David 2013; Goldkuhl 2012). This justifies the need for the researcher to understand the world from a subjective perspective of the participant rather than the objective observer of the action (Timans et al. 2019; Ponelis 2015). Proponents of

interpretivism are convinced that the use of this philosophy leads to findings that show many forms of acceptable reality about the phenomenon being studied (Babbie 2014; Gray 2013). This suggests that interpretivism could be a better philosophy than positivism to use in this study.

Unlike neutral positivist researchers, Zalaghi and Khazaei (2016) argue that the interpretive research process is subjective and it is important for researchers to acknowledge the role they play and how it influences the outcome of the research study. In this study, interpretivism could have enabled the researcher to interact with participants to understand their feelings and experiences of the factors which influenced the adoption of Cloud BI by SMEs. This could further have assisted the researcher to understand the problem through the meaning that decision-makers assigned to it. However, this philosophy has been criticised for being ineffective in determining intervention strategies (Kaushik & Walsh 2019; Kaur et al. 2013). Due to the nature of the problem, this empirical study required both qualitative and quantitative data at different stages. Therefore, a mixed-methods approach, best supported by pragmatism, was employed.

### **iii. Pragmatism**

Research in Information Systems (IS) is reported to have embraced pragmatism in practical research, theory and practical implications (Goldkuhl 2012; Mkansi & Acheampong 2012). Pragmatism is primarily concerned with practical solutions to existing problems because it focuses on actions, situations, and consequences instead of antecedent conditions (Alharahsheh & Pius 2020; Mkansi & Acheampong 2012; Creswell & Plano-Clark 2011). In this study, the existing problem was the lack of a user-friendly security evaluation framework for Cloud BI for use by SMEs, particularly in small towns where IT specialists are scarce. The security evaluation framework was to be proposed based on the findings of the empirical study. This justified the use of pragmatism because it was intended to assist the researcher to evaluate theories, experiences, feelings, and beliefs in terms of the success of their practical usage (Schoonenboom & Johnson 2017; Mkansi & Acheampong 2012).

Pragmatism rejects the notion of the absolute unit or single truth. Instead, it encourages researchers to view truth as what works in a situation at a particular moment (Kelly & Cordeiro 2020; Chandra et al. 2015). Therefore, the epistemology of pragmatism emphasises that the research is detached

from theoretical debates concerning the nature of truth and reality and concentrates on the practical understandings of tangible and real-world problems (Farjoun et al. 2015; Morgan 2014a). Because of this, pragmatism is viewed as an encouragement for researchers to critically examine the importance and meaning of the research data through its real-world significance (Akinbi 2015; Farjoun et al. 2015; Patton 2015; Morgan 2014a). Evidence emanating from some studies shows that pragmatism is helpful in organisational settings where the practice is closely linked to how knowledge is created (Kelly & Cordeiro 2020; Morgan 2014a). Researchers who utilise pragmatism in their organisational settings tend to move beyond objectivist conceptualisations when exploring and understanding the connections between knowledge and action in context (Farjoun et al. 2015; Morgan 2014b; Biesta 2010). This study was guided by a major research question which was divided into four sub-research questions on factors influencing the adoption of Cloud BI; strategies used; challenges faced in evaluating Cloud BI by SMEs, and aspects considered as vital in a security evaluation framework. The findings were used to provide a pragmatic solution to the study problem. Therefore, pragmatism was the most appropriate paradigm because it enabled the researcher to devise practical solutions to existing problems based on the affected SMEs.

Pragmatism was selected as the most appropriate research philosophy from those recommended by the Research Onion Model because the study incorporated both qualitative and quantitative strands in solving a practical problem. The advantage of using pragmatism was that it assumed a middle position between positivist and interpretive approaches (Kaushik & Walsh 2019; Goldkuhl 2012; Goles & Hirschheim 2012).

Researchers who advocate for the use of pragmatism cite several benefits. Scott (2016) purports that pragmatism is based on the willingness to change and an ability to respond to certain situations in which human beings inevitably find themselves. This means that researchers who undertake studies to solve real-life problems which the communities face are justified in adopting the pragmatic paradigm to achieve their objectives. The underlying philosophical assumptions of pragmatism promote mixed-methods research. The researcher can make use of different research methods and various data collection techniques in a single study and be able to evaluate their effectiveness (Scott 2016; Constantinides, Chiasson & Introna 2012; Saunders et al. 2012). The

mixed-methods design allows the researcher the freedom to select techniques for the collection and analysis of data based on the real-life realities of the affected population. The collected and analysed data, in turn, provide insight into the research questions. (Chandra et al. 2015; Creswell 2013). This research study sought to solve real-life problems. Placing the research problem at the centre of focus enabled the researcher to apply approaches that assisted in the understanding of the problem (Kelly & Cordeiro 2020; Cole, Purao, Rossi & Sein 2005). In this way, pragmatism as a research perspective stresses the priority of action over principles (Saunders et al. 2012), while advocating for ideas and practices to form the criteria of truth, rightness, and value that should be assessed and evaluated based on usefulness, workability, and practicality (Scott 2016; Constantinides et al. 2012).

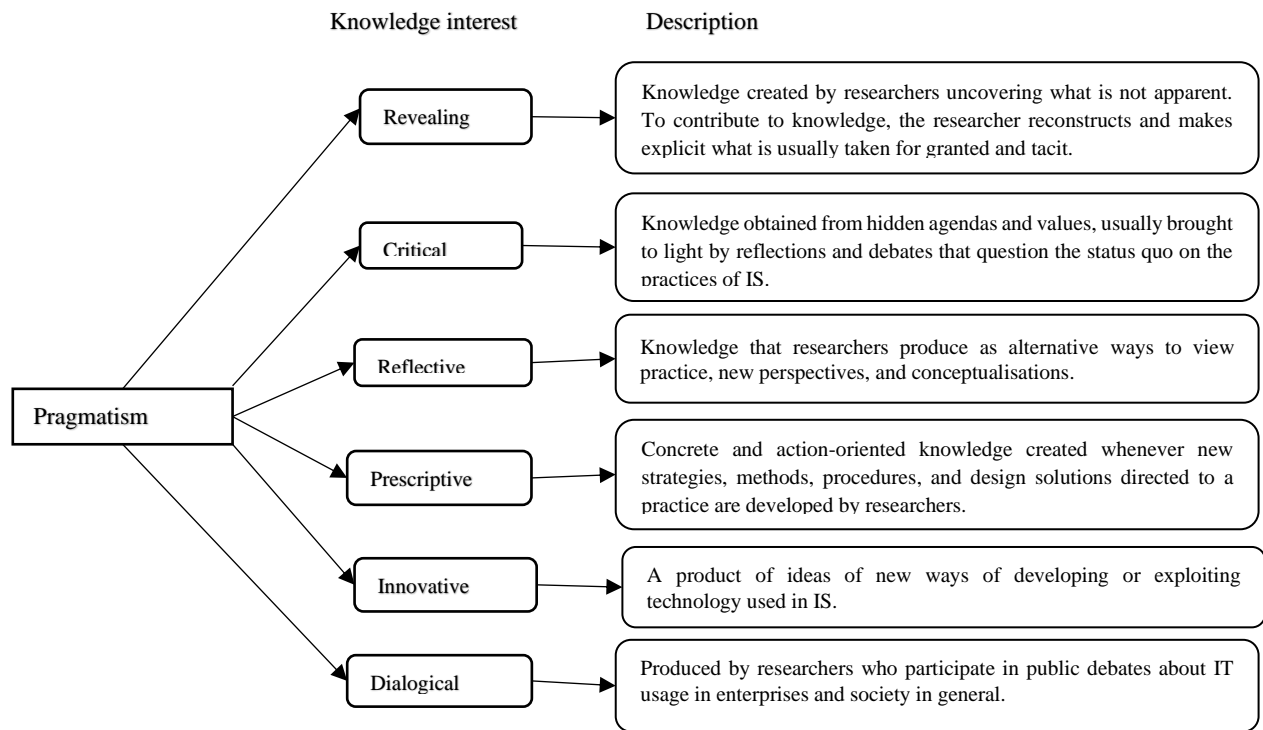
In this study, pragmatism was suitable for the study to answer research questions and provide a solution to a real-life problem. Instead of prescribing a security evaluation framework for Cloud BI, the researcher sought to use the findings of this study to propose a security evaluation framework, thus utilising the pragmatic approach. Pragmatism allowed the researcher to understand the practices of SMEs concerning the factors influencing the adoption of Cloud BI, evaluation of IT solutions and challenges faced.

Pragmatism encourages researchers to construct knowledge that stresses the usefulness of actions and change which is contrary to interpretivism, in which the knowledge claim is based on the interest of the researcher (Goldkuhl 2012). The types of knowledge that can be derived from the use of pragmatic research in IS are presented in the next subsection.

### **3.2.1.1. Knowledge in information systems research due to pragmatism**

The main purpose of IS research has been understood to be the generation and dissemination of knowledge, which contributes to the improvement of practice among practitioners (Morgan 2020; Chandra et al. 2015; Constantinides et al. 2012). Pragmatism provided the researcher with an opportunity to derive knowledge from what works in the social settings of SMEs in terms of Cloud BI security evaluation knowledge and skills. Goldkuhl (2012) identifies different knowledge types that researchers in IS can generate when using pragmatism, namely revealing, critical, reflective, prescriptive, innovative, and dialogical. Figure 3.3 shows different types of knowledge in IS.

However, this study intended to contribute to the four knowledge types proposed by Goldkuhl (2012), revealing, reflective, prescriptive and innovative.



**Figure 3.3: Types of IS knowledge derived from pragmatic research**  
Adapted from Goldkuhl (2012)

Literature shows that pragmatic researchers embrace both positivism and interpretivism research perspectives about theoretical knowledge when justifying the practical benefits to organisations and society gained from such knowledge (Senarathna et al. 2016; Chandra et al. 2015). Research studies that utilise pragmatism use the same research techniques used in positivism and interpretivism. The nature of the problem being addressed in this study led to the selection of pragmatism as the philosophy to use. While interpretivism is based on the SMEs' social meanings and interpretations of security in Cloud BI, pragmatism deals with how these interpretations and meanings could be used to propose an appropriate security evaluation framework. The prevailing notion about the adoption of Cloud BI is that what works for LBEs, works for SMEs, a problem researchable from an interpretive and pragmatist perspective. This study utilised functionalism to contribute to knowledge for action in the form of pragmatic knowledge, such as revealing, prescriptive, reflective, and innovative.

### **3.2.2. Deductive and inductive research approaches**

According to the ROM, deductive and inductive are the two research approaches used in several studies (Clohessy 2017; Venkatesh et al. 2013; Saunders et al. 2012). The comprehensiveness of deductive and inductive approaches to reasoning is confirmed by Gioia, Corley and Hamilton (2013). Literature shows that each of the approaches serves a different purpose that depends on the nature of the problem being solved and how the research study seeks to achieve that (Creswell & Cheryl 2018; Saunders et al. 2012). The deductive research approach is used for hypothesis testing after which the principle is either confirmed, refuted, or modified, while the inductive approach enables the researcher to undertake a research study based on observations or just an idea and let the theory be proposed at the end of the research study (Kaushik & Walsh 2019; Babbie 2014). Studies consider the deductive approach as being narrower because it emphasises testing and confirming hypotheses (Zalaghi & Khazaei 2016; Worster 2014). A study that uses a deductive approach is confirmatory because it is designed to confirm a preconceived idea or an anticipated association by testing the hypothesis (Creswell & Cheryl 2018). According to Olszewska et al. (2016), the deductive approach rigorously tests the validity of existing theories in real life by applying a set of techniques. The idea of a security evaluation framework for Cloud BI for SME decision-makers in South African small towns was novel, with unknown parameters and therefore, required the researcher to collect evidence on feelings, experiences, attitudes, and behaviour of decision-makers on challenges that led to poor adoption and use of Cloud BI. At the beginning of the research study, the factors influencing the adoption of Cloud BI among SMEs, the strategies used to evaluate these technologies, and the challenges faced were unknown, and this made the deductive approach unsuitable.

Eriksson and Kovalainen (2015) posit that an inductive study is concerned with a pattern of observation and the development of descriptions of theories with hypotheses. Furthermore, in an inductive study, theories or hypotheses are usually applied at the late stage of the research, and the researcher is free to change the direction of the research process (Schoonenboom & Johnson 2017; Eriksson & Kovalainen 2015; Worster 2014). Creswell (2013) describes an inductive study as being exploratory and the interests of the researcher are to describe or explain important issues using several research techniques. Creswell (2014) encourages researchers to utilise an inductive approach if existing knowledge about the problem being solved is limited. In this study, the use of

the inductive approach was intended to enable the researcher to propose the framework from the findings of data collected from decision-makers of SMEs. Inductive research uses a bottom-up approach as it starts with observations which result in a broader and generalised theory. This illustrates that an inductive approach is useful for identifying anomalies and patterns that ultimately culminate in the formulation of possible hypotheses, models, and a framework to provide the needed solution to the existing problem.

The purpose of the study was to propose a security evaluation framework based on the SME decision-makers' views and understanding of the evaluation of IT solutions, including Cloud BI, strategies used, and the main considerations of the evaluation process. The reason for adopting an inductive approach was to enable the researchers to collect evidence about decision-makers' views and experiences of factors influencing the adoption of Cloud BI and how they evaluated the applications. Subsequently, the study proposed a security evaluation framework based on empirical findings (Schoonenboom & Johnson 2017; Worster 2014). According to Jebreen (2012), the advantages of the inductive approach are that:

- it makes it easy to combine and summarise different raw data in a single study;
- it enables the researcher to create clear links between research objectives and the results used to communicate the findings and conclusions of the study to others; and
- it assists in the development of a theory or expansion of knowledge based on the experiences and processes revealed by different forms of data.

The inductive approach provided the researcher with an opportunity to use findings from responses from research participants to propose a security evaluation framework for Cloud BI appropriate for SMEs in under-resourced South African towns.

### **3.2.3. Research design**

A research design is a framework used to address different aspects of the research study, from problem identification to detailed data collection and analysis techniques (Creswell 2014; Worster 2014). A research design connects empirical data collected to the theoretical arguments posed in the research study (Zefeiti & Mohamad 2015; Saunders et al. 2012; Churchill 1979). Literature shows that the three commonly used research designs are quantitative, qualitative, and mixed-methods, each selected depending on the research problem; questions to be answered; the types of

data to be collected; and how said data were to be analysed (Timans et al. 2019; Omair 2015; Creswell 2014; Al-Yaseen 2012). This implies that each design serves a specific purpose in a research study and the researcher needs to consider each of them carefully.

### **i. Quantitative designs**

Quantitative designs are used in quantitative research whose purpose is to establish objectivity in the provided facts, accurately predict events, and formulate findings in the form of laws generalisable to large populations (Babbie 2014; De Villiers 2012). Quantitative designs are popular in natural sciences where most research takes the form of experiments in laboratories where variables are controllable (Luís, Erdmann, Hörner & Meirelles 2020). Studies that use quantitative designs collect numeric data or data that can be changed to numbers and then analysed statistically (Myers & Avison 2011). Quantitative research applies quantitative design to identify general trends in selected populations by applying quantitative techniques to determine the size, amount, or magnitude (Punch 2013; Myers 2009). According to Oates (2006), quantitative designs lead to the use of surveys and experiments as data collection techniques and eventually apply statistical analysis whose main purpose is to determine what should be measured and counted. Quantitative designs are used in studies to support the positivist epistemological stance in which the research phenomena are being studied and the researcher is expected to be an independent object and does not influence the outcome of the study.

### **ii. Qualitative designs**

Qualitative designs are used to assist researchers to plan studies to collect qualitative data conveyed as words, text and actions and analyse it qualitatively (Maxwell 2013; Denzin & Lincoln 2011). Qualitative designs are commonly used in social science studies which focus on human behaviour and belief phenomena (Babbie 2014; Marshall & Rossman 2014). By using a qualitative design, a researcher can study participants closely in their natural environments, analyse the words, actions, and motivations conveyed, then report on feelings, social situations, and experiences in real-world settings (Creswell 2013; Maxwell 2013). In this context, a qualitative design was used to select research techniques that enabled data collection by prioritising situations in which participants were comfortable, in an inductive, interactive, and flexible manner (Creswell 2014; Osborn 2014). Furthermore, Myers (2020) asserts that researchers who intend to study social and



cultural problems in depth tend to apply qualitative designs. Data collection methods used with qualitative designs include observations, interviews, fieldwork, and focus groups in which the researcher can be actively involved (Moen & Middelthon 2015; Creswell 2014). Data analysis techniques used in qualitative studies tend to be narrative, thematic and content analysis, which are mostly subjective, with the researcher and the participants deeply involved (Castleberry & Nolen 2018; Nowell, Norris, White & Moules 2017; Braun & Clarke 2006).

Qualitative research approaches are reported to have limitations in that they focus on meanings and participants' experiences, ignoring contextual sensitivities (Rahman 2017; Silverman 2010). Qualitative approaches are criticised for using small sample sizes, sample bias and intrusiveness of the researcher (Venkatesh et al. 2013; Constantinides et al. 2012). Small sizes in qualitative studies restrict generalisation to large populations, while sample bias raises issues of representativeness. Researchers using qualitative designs are criticised for interfering with the participants during data collection (Llave 2017; Momani & Jamous 2017). These limitations were taken into consideration during the selection of the design.

### **3.2.3.1. Mixed-methods research designs**

Mixed-methods designs have been successfully used to solve problems in IS research because they allow researchers to utilise both qualitative and quantitative data collection and analysis techniques and this provides better insights into the research problem than either design separately (Timans et al. 2019; Creswell & Creswell 2018; Schoonenboom & Johnson 2017). According to Cameron (2015), mixed-methods designs emphasise that a researcher treats a selected problem in a manner that might not be possible with a quantitative or qualitative design alone. Several studies show that mixed-method designs are driven by pragmatism instead of principles (Moen & Middelthon 2015; Venkatesh et al. 2013). Researchers who adopt mixed-methods designs seek to overcome deficiencies of using a quantitative or qualitative when dealing with a novel research problem (Punch 2013; De Villiers 2012).

To use a mixed-method design, some studies recommend that one of the following four requirements is apparent: 1) very little is known about the problem being researched, and a qualitative approach is required before a quantitative approach is employed; 2) the findings of a

research approach are better understood by utilising the findings of another approach; 3) a single research approach cannot provide meaningful findings; and 4) the findings made in the quantitative approach enriched those from the qualitative approach (Luís et al. 2020; Maxwell 2013; Punch 2013). In this study, the security evaluation of Cloud BI by SMEs in South African small towns was an area that has not been explored by existing studies.

By using mixed-methods designs, the researcher was free to choose data collection and analysis methods that provided insights into the research questions without being loyal to a certain theoretical framework (Creswell & Cheryl 2018; Chandra et al. 2015). According to Cameron (2015), the use of mixed-methods research designs allows the researcher to collect, analyse, and interpret qualitative and quantitative data in a single study. Schoonenboom and Johnson (2017) posit that the rationale of using mixed-methods research is to expand and strengthen the conclusions of a research study and to contribute to the publishable literature by answering research questions incorporating both qualitative and quantitative techniques. Venkatesh, Brown and Bala (2013) posit that IS researchers who utilise mixed-methods research designs can have a better understanding of the problem being studied and be able to develop new theoretical ideas for future applications. Ultimately, the mixed-methods design was chosen to provide a better understanding of the current practices of decision-makers during the security evaluation of Cloud BI, which would support the proposal of a framework to assist SMEs to overcome the challenges faced when evaluating Cloud BI.

The presence of several mixed-methods designs allowed the researcher to select the most appropriate design compatible with the phenomenon being studied and the research philosophy being used. When selecting a mixed-methods design from the six variations, it is encouraged that time distribution, weight attribution, combination, and theorisation be considered (Luís et al. 2020; Creswell & Cheryl 2018).

*Time distribution* requires one to decide whether both quantitative and qualitative data should be collected simultaneously (concurrent) or in stages (sequential) (Luís et al. 2020; Creswell & Plano-Clark 2011). For this study, data were collected sequentially, starting with qualitative data and then quantitative data. This required the study to address the weight attribution of the data collection techniques (Luís et al. 2020; Maxwell 2013). *Weight attribution* was important in determining

which component of the study, quantitative or qualitative was given more priority (Luís et al. 2020; Creswell 2014; Punch 2013). For this study, weight attribution prioritised the qualitative strand in which data were collected from SME decision-makers in their natural environment, the workplaces. The *combination* aspect determined whether the data were to be treated separately or mixed; and when and how the mixing was to occur (Creswell & Plano-Clark 2011; Cathain, Murphy & Nicholl 2007). For this study, the findings from the qualitative phase were integrated with the results from the quantitative phase during the interpretation stage, as recommended by literature from various sources (Timans et al. 2019; Hughes 2016). According to Luís et al. (2020), the implementation of a mixed-method design needs to be aligned with the *theoretical perspective* used in a particular study. Mixed-methods approaches are grounded in pragmatism (Creswell & Cheryl 2018; Creswell & Creswell 2018; Cameron 2010, 2015). The problem being solved by this study required the use of the mixed-methods design within the pragmatism philosophical perspective.

When using mixed methods designs, researchers always face challenges in attributing weight to qualitative and quantitative results which are compounded by time management (Luís et al. 2020; Mihas, Creswell & Plano-Clark 2019). In this study, the weight attribution for qualitative data was more than that of the quantitative data and more time was spent in collecting and analysing qualitative data. This implies that quantitative results were used to corroborate qualitative findings.

Creswell (2013) uses the above four factors to categorise mixed-method designs into six strategies, namely, concurrent triangulation, concurrent nested, concurrent transformative, sequential explanatory, sequential exploratory and sequential transformative. Table 3.2 is a comparison of the mixed-methods designs based on the characteristics, purpose and how suitable each of them was in this study. Creswell and Creswell (2018) identified two types of sequential mixed methods as exploratory and explanatory, with each designed to serve a different purpose. According to Luís et al. (2020), the type of sequential mixed-method strategy used depended on the initial idea of the researcher and the type of data collected first.

The major research question for this study was: *What are the main components of a security evaluation framework for Cloud BI suitable for small and medium enterprises in under-resourced small South African towns?* To answer this research question, qualitative data were collected first

to explore the problem of interest of participants in their natural settings and later the findings were employed to design a questionnaire to collect quantitative data from a larger sample. This was intended to verify and corroborate the findings of the initial phase and subsequently, propose a security evaluation framework. Creswell and Cheryl (2018) refer to such a strategy as exploratory sequential because the initial idea of the researcher is to explore the problem with a small sample to identify variables that can be further researched in the later stage of the study. Furthermore, authors, such as Creswell and Cheryl (2018) and Creswell and Creswell (2018) emphasise the use of exploratory sequential mixed methods if the problem is novel and cannot be solved by applying either qualitative or quantitative design. Mixed methods design, characteristics, purpose, and suitability are present in Table AP3.1 in *Appendix H*.

To select the most appropriate strategy, each sub-research question was compared with the characteristics and purpose of each mixed-methods design (see Table 3.2). Table 3.2 shows that the types of data required by each SRQ justify the selection of the exploratory sequential strategy. Due to the exploratory and developmental nature of the study, the exploratory sequential mixed-methods was selected from the six mixed-methods designs recommended by Creswell and Creswell (2018) and Creswell and Cheryl (2018). The design was selected for its strength in allowing the researcher to collect and analyse data in two separate phases, the qualitative (QUAL) and quantitative (QUAN) phases. Exploratory sequential design is reported to be useful in studies where researchers seek to design and test a new instrument that can be used to solve the existing problem (Mihás et al. 2019; Creswell & Cheryl 2018; Creswell & Creswell 2018). In this case, a security evaluation framework for SMEs was to be proposed based on the findings of the case study and the best practice from the industry frameworks and standards. The philosophical assumptions behind the exploratory sequential design were that the research problem and purpose of the study required the qualitative method to have greater priority within the design than the quantitative method (Mihás et al. 2019; Creswell & Cheryl 2018; Creswell & Plano-Clark 2011).

**Table 3.2: Determination of suitability of design based on research questions**

| Sub-research question  | Data needed                 | Sequential design          |
|--|-----------------------------|----------------------------|
| <b>SRQ1:</b> What factors influence the adoption and use of Cloud BI among SMEs in under-resourced South African towns?                                | QUALITATIVE<br>Quantitative | EXPLORATORY<br>Explanatory |
| <b>SRQ2:</b> How do small and medium enterprise decision-makers evaluate Cloud BI before adoption?   | QUALITATIVE<br>Quantitative | EXPLORATORY<br>Explanatory |
| <b>SRQ3:</b> What challenges do small and medium enterprise decision-makers face when evaluating Cloud BI?   | QUALITATIVE<br>Quantitative | EXPLORATORY<br>Explanatory |
| <b>SRQ4:</b> What do decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises? | Qualitative<br>QUANTITATIVE | Exploratory<br>EXPLANATORY |

Research studies that utilise exploratory sequential mixed-methods are reported to have benefited the generalisation of qualitative findings to a larger sample than that used in the research study (Creswell & Creswell 2018; Schoonenboom & Johnson 2017; Cameron 2015). This study used the findings of an interview with a small sample to develop a questionnaire to collect data from a larger sample of SMEs and to propose a security evaluation framework for Cloud BI. For example, Hamshire, Spearing and Wibberley (2013) conducted an exploratory sequential mixed-methods study through interviews with a sample of sixteen nursing students to understand experiences and expectations of their nursing programme. The authors used the findings to develop an online survey questionnaire which was then administered to 1080 student nurses across nine UK universities. Similarly, this study used the findings from the interview of a small sample of decision-makers to design a questionnaire and distribute it to a larger sample of SME decision-makers. The questionnaire sought information about experiences, beliefs, and feelings; of factors affecting the adoption of Cloud BI by SMEs; strategies used in security evaluation; and challenges faced by SMEs decision-makers in five selected towns in Limpopo.

This study collected data sequentially, starting with qualitative data, using semi-structured interview methods in the QUAL phase, whose results were used to provide insights into factors that influenced SMEs to adopt Cloud BI, the current practices and efforts employed by SMEs in selecting Cloud BI, and the challenges faced. In the QUAN phase, quantitative data were collected using a survey questionnaire developed from the findings of the QUAL. The results were used to explain the trends emanating from the previous data analysis. The findings from both phases were used to propose a security evaluation framework for Cloud BI.

### **3.2.3.2. Variants of an exploratory sequential mixed-methods design**

The two types of exploratory sequential mixed-method design are theory development and instrument development (Akinbi 2015; Creswell & Plano-Clark 2011). Literature suggests that the qualitative strand is carried out when developing a new theory or hypothesis in which the researcher examines the occurrence of the findings and/or testing the theory with a large sample (Creswell & Creswell 2018). For this study, the instrument-development variant was used to propose an instrument needed to solve an existing problem, in this case, a security evaluation framework for Cloud BI, using findings from the empirical study of SMEs from five towns in the Limpopo Province. According to Mihas et al. 2019, exploratory sequential mixed methods as a design seeks to combine qualitative and quantitative data collection and analysis in a sequence of two phases. In the first phase of the exploratory sequential mixed-methods design, qualitative data was collected and then analysed to generate themes and an instrument used in the QAUN phase (Mihas et al. 2019; Berkowsky et al. 2017).

The proponents of exploratory sequential design, provide three basic reasons for the utilisation of this design, namely: 1) the absence of the instruments for use in an area of study; 2) variables being investigated not known to the researcher(s); and 3) lack of theory or model as a guide in the area being investigated (Cameron 2015; Creswell 2014). For this study, there was a literature gap in the security evaluation of Cloud BI by SMEs in South Africa; neither the types of knowledge in security evaluation decision-makers had nor how they evaluated security in Cloud BI was clear. The use of the exploratory sequential design was based on the reasons stated above.

### **3.2.4. Exploratory sequential mixed-method research strategy**

The research strategies used in this study depended on the two phases of the data collection and analysis, namely QUAL and QUAN. According to Creswell and Plano-Clark, (2019), the exploratory sequential mixed-methods strategy combines qualitative and quantitative data collection and analysis in a sequence of phases. An exploratory qualitative survey was a valuable means to understand what was happening, to seek new insights, ask questions, and assess the phenomenon in a new light (Creswell & Plano-Clark 2011). Another main advantage of the exploratory survey strategy was its flexibility as it allowed the researchers to use different data collection methods within the same research (Carcary et al. 2014; Saunders et al. 2012; Yin 2012).

The exploratory sequential approach was used to explore the problem to determine the variables to be measured in the QUAN phase (Mihás et al. 2019; De Villiers 2012). In the QUAL phase, qualitative data was collected, and the analyses produced themes and sub-themes which were used to produce a survey questionnaire to use in the QUAN phase to collect quantitative data, which could be a survey or any other form of quantitative data collection.

### **3.2.5. Population, sample size and sampling procedures**

The specifications of the population, sample size and sampling procedures for this study are provided in the subsections of this section. In SMEs, decision-makers are responsible for the selection and use of various IT systems and therefore, they are in the best position to provide the information on the security evaluation of Cloud BI. Similarly, IT security specialists know various cloud applications and can evaluate the proposed security framework. Therefore, data were collected from three samples, two from SME decision-makers and the other from IT security specialists.

#### **i. Population**

The population of this study consisted of SME decision-makers who used IT information systems to support their business operations. The target population comprised all individual SME decision-makers whom the researcher was interested in to generalise the findings of a scientific inquiry (Cohen, Manion & Morrison 2018; Creswell & Creswell 2018). According to Denzin and Lincoln (2011), population specifications in qualitative and quantitative studies are dictated by different principles because each study depends on different types and sizes of samples. Baskarada (2014) argues that qualitative research studies usually focus on relatively few participants who describe their experiences, beliefs, perceptions, and/or knowledge of the research questions or phenomenon being studied.

On the other hand, quantitative studies require the participation of a relatively large number of individuals who are not required to extensively describe experiences of the phenomena (Creswell & Cheryl 2018; Baskarada 2014). This implies that qualitative and quantitative designs utilise different procedures and criteria in selecting population members, thereby making the target and accessible population different in these studies (Asiamah, Mensah & Oteng-Abayie 2017; Hooda

2014). This study utilised the exploratory sequential design to benefit from the procedures and criteria in selecting population members for qualitative and quantitative designs (Creswell & Cheryl 2018; Creswell & Creswell 2018). Both QUAL and QUAN phases of this study utilised the same target population of SME decision-makers but different samples, sample sizes, sampling procedures, data collection, and analysis techniques.

The target population for this study consisted of all SME decision-makers from five selected towns in Limpopo Province who were utilising online IT systems, web, and Cloud BI to support their business operations. The five towns were: Giyani, Louis Trichardt, Mokopane, Musina and Thohoyandou.

#### ii. **Samples and sample size**

The main function of a sample in the study was to allow the researcher to conduct the study with individuals from the accessible population, to generalise the findings (Preece & Bularafa 2015), and to propose a security evaluation framework for SMEs from five selected towns in Limpopo Province. In a study dealing with people, a sample becomes a set of respondents, participants, informants, or subjects, depending on the type of study (Schoonenboom & Johnson 2017; Carcary et al. 2014). In this study, the term *participants* was used for individuals in the sample for the QUAL phase, and *respondents* were individuals in the sample for the QUAN phase respectively (Cohen et al. 2018). Each sample provided different types of data in the phase it was used.

The sample size for the QUAL phase was thirteen (13) SME decision-makers, determined by data saturation (De Villiers 2012). The QUAN phase sample comprised fifty-seven (57) SME decision-makers, based on the completed and returned questionnaires.

#### iii. **Sampling procedures**

The sampling procedures used in this study depended on the type of data and sample size needed. The sampling procedures are described in the respective phases of the study.

### **1. Sampling for Qualitative phase**



The QUAL phase provided the researcher with a chance to understand the subjective reality of the participants from their views, feelings, and experiences of factors influencing the adoption of Cloud BI, their understanding of security evaluation, and how they evaluated the technology (Gentles, Charles, Ploeg & McKibbin 2015). The literature emphasises that researchers should identify the members of populations who can provide rich, descriptive accounts of the topic being explored (Roulston 2018; Patton 2015). Interviewing was one of the primary data collection methods, thereby compelling the researcher to find participants who could provide a good description of the phenomenon being studied and were prepared to spend their time elaborating with a researcher on the topic (Patton 2015; Rubin & Rubin 2012). The QUAL phase used qualitative data from a purposive sample of SME decision-makers using IT systems who were interested in adopting Cloud BI. Ilker, Sulaiman and Rukayya (2016) argue that purposive sampling allows the researcher to purposefully choose participants based on the qualities needed in that study. By using purposive sampling techniques, the researcher was able to decide what should be known, and then choose participants who could provide the information based on their beliefs, perceptions, experience, feelings and knowledge of the phenomenon being studied (Cohen et al. 2018; Creswell & Cheryl 2018; Leedy & Ormrod 2015).

## **2. Sampling for Quantitative Phase**

The QUAN phase utilised quantitative data from a convenience sample of 57 decision-makers, collected using postal and online survey questionnaires. Convenience sampling is a nonprobability sampling technique whereby members of the target population who met the required practical criteria, including easy accessibility, geographical proximity, availability at a given time, and the willingness to participate, are included in the study Etikan, Sulaiman and Rukayya (2016). The advantages of convenience sampling in this study were affordability and ease to get readily available respondents to complete the questionnaires (Etikan et al. 2016; Gentles et al. 2015). Convenience sampling is the most popular strategy used in developmental research because it is fast, easy, least time-intensive, and least expensive to implement. According to Etikan et al. (2014), convenience samples are useful in situations in which:

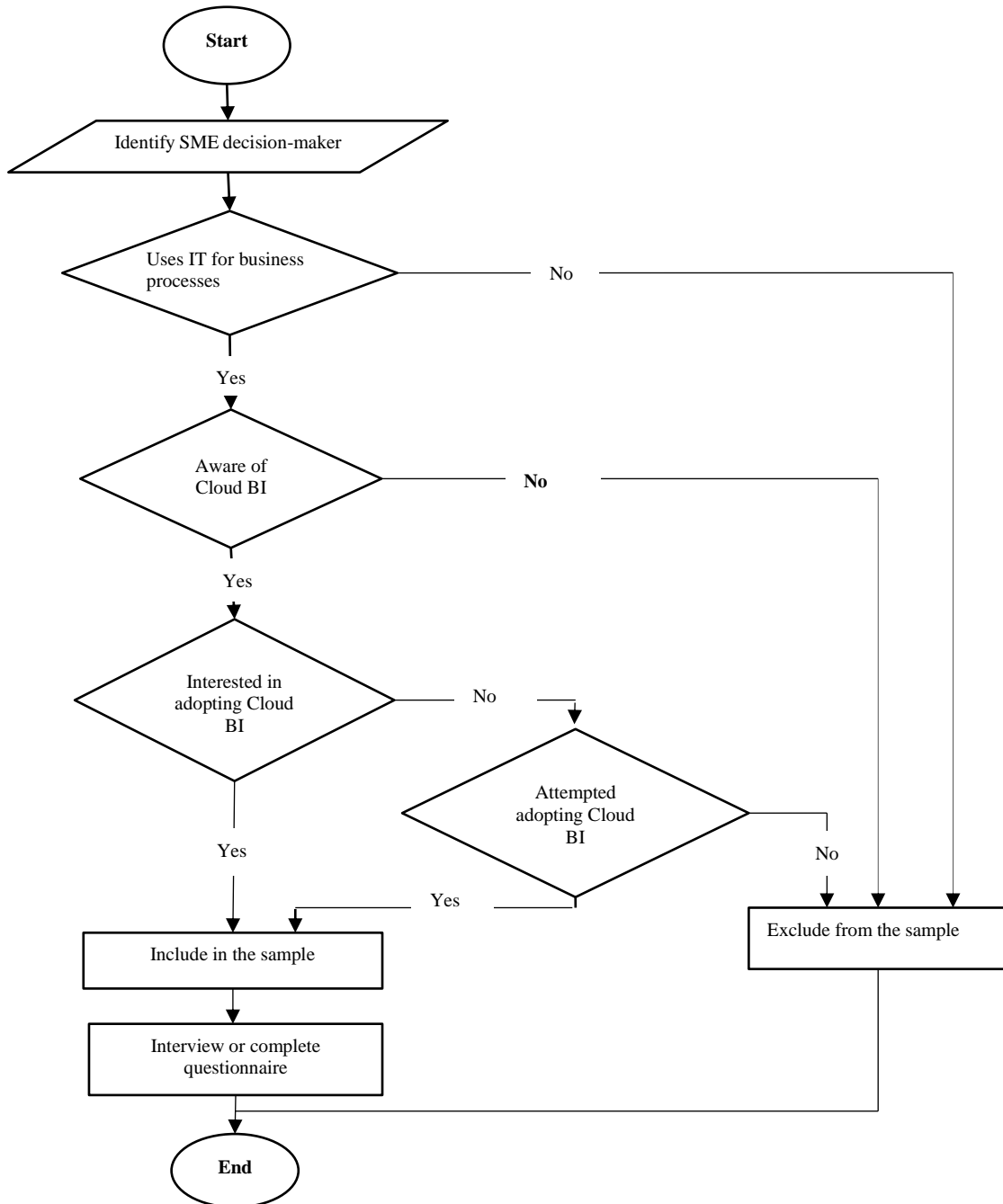
- the research population is difficult to define;
- the sampling unit is not clear due to the unavailability of a sampling frame;
- there is no complete source list to use;

- the target population is widely dispersed, and other sampling techniques are not efficient in collecting data; and
- the study is exploratory, and its purpose is to have insights into the problem being studied.

In this study, the number of SMEs who used IT and contemplated adopting and utilising Cloud BI was unknown, which justified employing convenience sampling in the QUAN phase. The sample depended on the availability of SME decision-makers and their eagerness to participate in the study.

iv. **Inclusion and exclusion criteria**

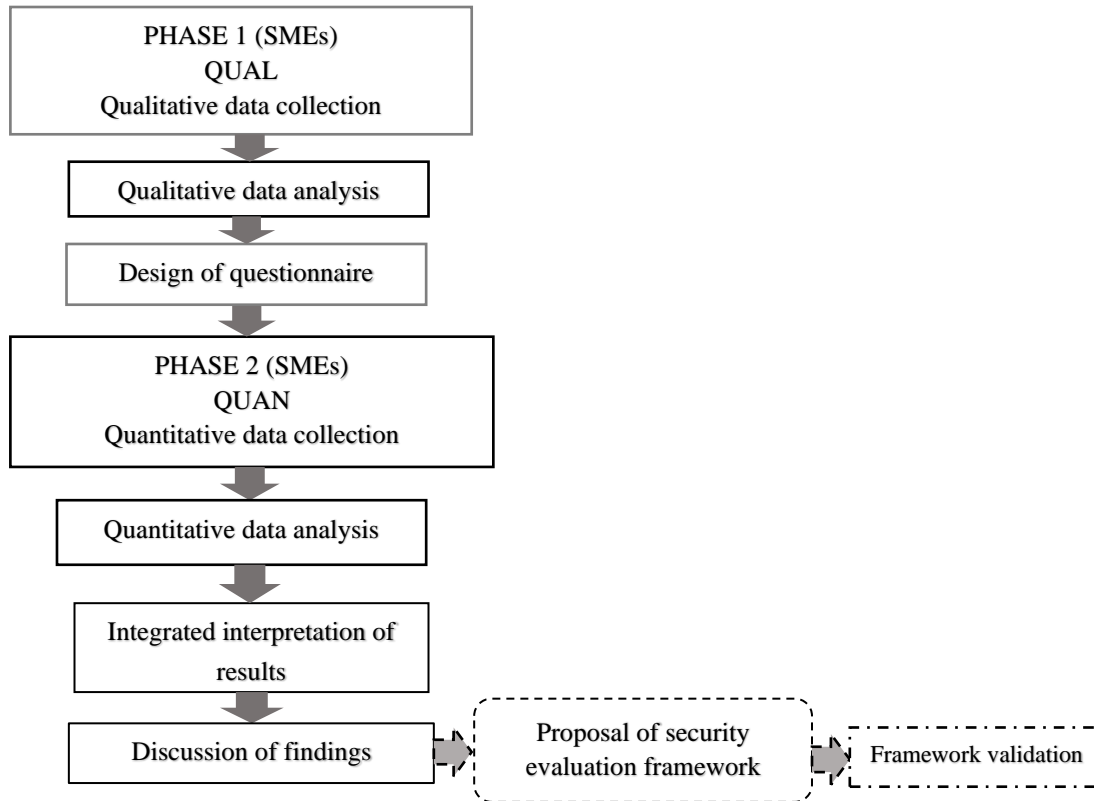
The process of including and excluding decision-makers enabled the selection of participants who met the requirements of online IT systems usage and Cloud BI awareness and adoption interests. Figure 3.4 shows the inclusion and exclusion criteria used. The strategy was successfully employed in the selection of the samples for the QUAL and QUAN phases respectively. For an individual decision-maker to be a participant, must first fulfil several criteria, such as being a user of IT systems in supporting the business operation, awareness of Cloud BI, interested in adopting or already adopted Cloud BI. In the process, those individuals who satisfied the requirements were interviewed telephonically or in person. This was applied to the questionnaire method.



**Figure 3.4: Inclusion and Exclusion criteria**

### 3.2.6. Data generation and analysis methods in exploratory sequential design

This study followed the data collection and analysis for an exploratory sequential design, and the practical research steps shown in Figure 3.5, adapted from Creswell and Plano-Clark (2011). The model shows that in each stage data were collected, analysed, and then integrated during the interpretation.

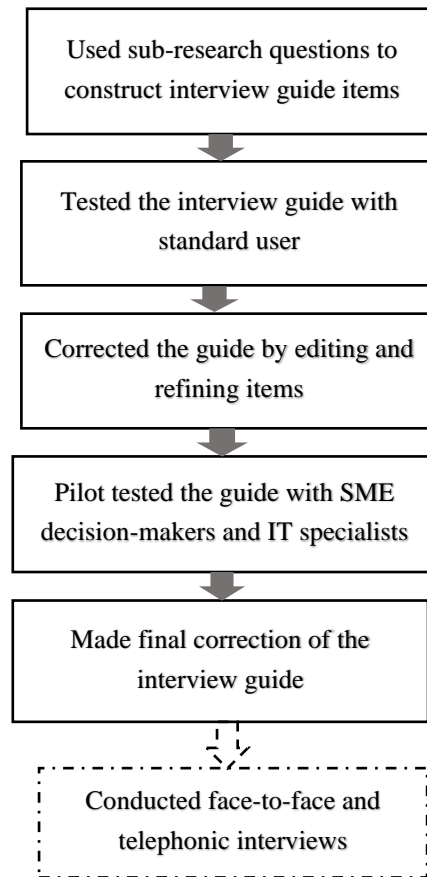


**Figure 3.5: Exploratory sequential mixed-methods data collection and analysis**  
 Source: Creswell and Plano-Clark (2011) model adapted for this study

The empirical stage of the exploratory sequential mixed-method research is characterised by the multiple steps of instrument design and data analysis as shown in Figure 3.5, elaborated in the subsequent sections.

**i. Qualitative Phase: Instrument development and pilot-testing**

The development of the interview guide was guided by the objectives and research questions stated in Chapter 1. The interview questions were designed to solicit information from decision-makers regarding which Cloud BI applications to adopt, the factors influencing the adoption process, the evaluation strategies used, and challenges faced, as well as major components of the security evaluation framework. Figure 3.6 shows stages in the development of the interview guide which was adapted from Seidman (2012) and Rubin and Rubin (2012).



**Figure 3.6: Steps in designing and pilot testing a semi-structured interview**  
Adapted from Seidman (2012) and Rubin and Rubin (2012)

The questions in the semi-structured interview guide were derived from SRQs. The interview guide was pilot-tested with three decision-makers. The interview guide was then revised using ideas from an experienced interviewer and feedback from the three participants. The final interview guide is in *Appendix E*.

ii. **Data collection in qualitative phase using semi-structured interviews**

Interviews have been used in several studies and are confirmed as an effective means of accessing participants' views, feelings, beliefs, experiences, and interpretations of actions and events taking place within their confines (Creswell & Cheryl 2018; Leedy & Ormrod 2015; Yin 2012). Some studies encourage the use of the interview method because of its added advantage of facilitating direct interaction of the researcher and individual participants on a one-to-one basis; this enables

the researcher to extract relevant information about the phenomenon (Kaushik & Walsh 2019; Ibrahim & Musah 2015). The interview method was used to facilitate the researcher to gather data on factors influencing the adoption of Cloud BI and security evaluation, to answer research questions, and to propose a security evaluation framework for Cloud BI.

The semi-structured interview guide in *Appendix E* was used for interviews with a sample of 13 decision-makers in SMEs. Rubin and Rubin (2012) and Roulston (2014) are of the view that semi-structured interviews can provide the interviewer with an opportunity to ask similar questions in such a way that participants can freely generate meaningful descriptions of the phenomenon in their own words.

Before the interview sessions, all interviewees were briefed about the purposes of the study and were asked for their consent to be interviewed. Some interview sessions were held face-to-face at places convenient to the interviewees, while other interviews were conducted telephonically. Permission for recording the interview sessions was obtained from each interviewee. Participants were requested to sign the informed consent form before the interview sessions. On average, each interview session lasted 25 to 35 minutes long, with face-to-face being longer than telephonic ones. All interviews were conducted in English. The researchers stopped conducting interview sessions when there were more similarities in the ideas expressed by incoming interviewees than new ideas (saturation). Saturation is described as information redundancy (Ando, Cousins & Young 2014) or gathering data to a point where no new information is generated (Braun, Clarke, Hayfield & Terry 2019). The use of a sample of 13 in this study was based on Namey, Guest, McKenna and Chen (2016), who argue that data saturation in qualitative studies using interviews can be achieved with between 5 to 12 participants. The interview recordings were stored in a DVD and USB for backup and can be made available on request. Soft copies of transcriptions can be availed if needed.

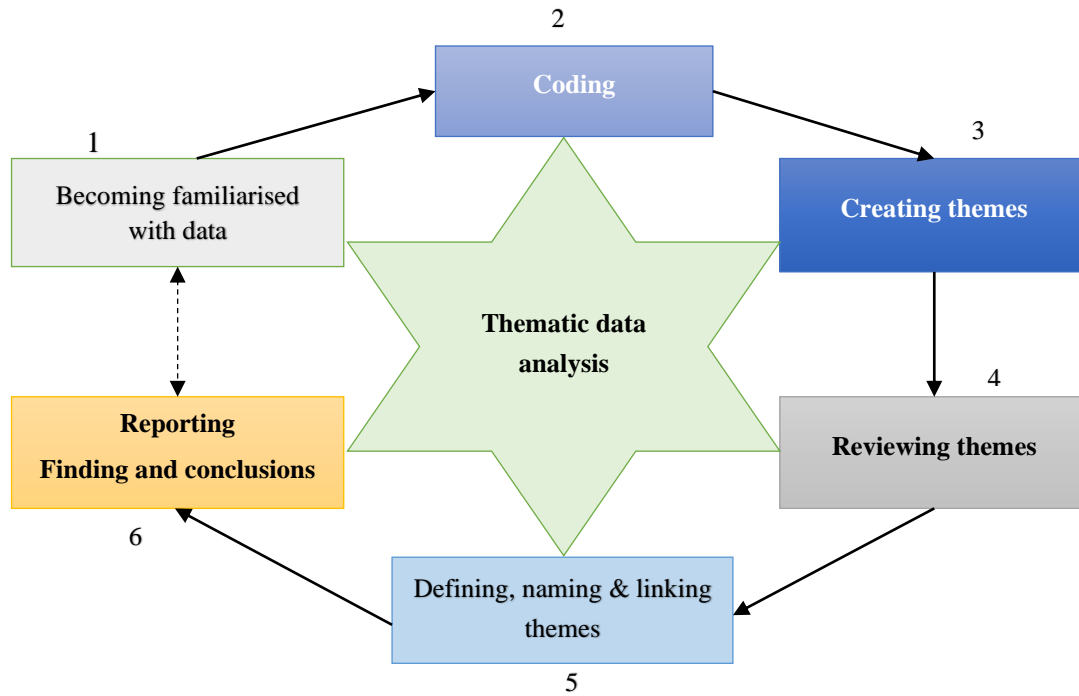
### iii. **Qualitative data analysis**

According to Creswell and Plano-Clark (2019), qualitative data analysis is a process of identifying meaningful quotations, using appropriate topics to code them, and formulating themes. Guest, MacQueen and Namey (2012) posit that qualitative data are text and words that a researcher has to analyse to determine what the participants' feelings, experiences, beliefs, knowledge, and

behaviour mean. Qualitative data analysis involves reducing data, in-text and words, to codes to represent themes or concepts and this process may use quantitative techniques to determine patterns in the relations among the codes (Castleberry & Nolen 2018; Guest et al. 2012). Braun and Clarke (2014) and Braun, Clarke, Hayfield and Terry (2019) view a theme as representing something important about the data regarding the research questions and a type of patterned response or meaning within the data set.

All interviews were transcribed by listening to the audio repeatedly, making notes, and identifying key statements. After transcribing the interviews, a file was created for each transcript in Microsoft Word, then imported to Atlas.ti8, where the thematic analysis was used in qualitative data analysis. Maguire and Delahunt (2017) posit that thematic data analysis should involve the identification of patterns or themes in a given qualitative data set. Literature shows that thematic analysis is a basic method used to provide important skills for conducting qualitative data analysis (Castleberry & Nolen 2018; Nowell et al. 2017; Braun & Clarke 2014). Several studies which used thematic data analysis found it simple and free from any theoretical or epistemological perspective (Maguire & Delahunt 2017; Nyalungu 2011). This study utilised the thematic framework for qualitative data analysis following the Braun and Clarke (2006) and Clarke and Braun (2013) model shown in Figure 3.7. The framework comprises six steps that a researcher should follow for successful data analysis.

*Data familiarisation* initiated the thematic data analysis process (Morgan & Nica 2020; Braun & Clarke 2014; Clarke & Braun 2013). The researcher became familiarised with the data by repeatedly scrutinising the transcripts as well as listening to the audio recordings to make sure that the important facts were extracted. The researcher thoroughly examined the main thoughts, views, and experiences expressed by the interviewees and started identifying and labelling similar ideas from the meanings conveyed by the narratives. Atlas.ti8 package made this exercise manageable by making it easy for the researcher to move forwards and backwards, comparing ideas from different transcripts.



**Figure 3.7: Six steps for thematic data analysis**  
Adapted from Braun and Clarke (2006)

*Initial coding* occurred in the second step of the thematic analysis in which the researcher identified preliminary codes to label interesting and meaningful ideas, a recommendation made by Castleberry and Nolen (2018). To manage initial coding, Maguire and Delahunt (2017) suggest that data should be summarised methodically into smaller analysable units by creating categories and concepts derived from the data. In the context of this study, the initial labelling of ideas produced several codes which needed further scrutiny. The researcher reduced the codes after reading through the transcripts several times, thoroughly analysing and comparing the ideas. Figure 3.8 shows a sample of the codes.



| RQ | Name  | Grounded | Density | Groups                             |
|----|---|----------|---------|------------------------------------|
| RQ | Belief:   | 0        | 0       | [RQ1a: Belief on the importance of |
| RQ | Belief: Cloud as future data storage                                      | 1        | 0       | [RQ1a: Belief on the importance of |
| RQ | Belief: I remain sceptical about using CBI                                | 1        | 0       | [RQ1a: Belief on the importance of |
| RQ | Belief: Importance of safety when using technology                        | 1        | 0       | [RQ1a: Belief on the importance of |
| RQ | Belief: On CBI Improves decision making                                   | 5        | 0       | [RQ1a: Belief on the importance of |
| RQ | Belief: Skills requirement by managers in IT and CBIs                     | 1        | 0       | [RQ1a: Belief on the importance of |
| RQ | Belief: The cloud as a suitable replacement for on-premise infrastructure | 2        | 0       | [RQ1a: Belief on the importance of |

**Figure 3.8: Sample of coding for belief**

To *search for themes*, the researcher grouped all similar codes into themes leading to interpretive analysis (Nowell et al. 2017; Salum et al. 2016). To facilitate easy categorisation, the researcher sorted all relevant data extracted according to the main themes and sub-themes.

During the *reviewing themes and sub-themes* step, the researcher critically compared, contrasted, and decided whether to combine, refine, separate or discard the initial themes (Morgan & Nica 2020; Braun & Clarke 2014; Clarke & Braun 2013). In this study, this step was critical in that it required the themes to be matched with each of the 4RQs.

*Defining, naming, and linking themes to research questions* was the penultimate step in the thematic analysis in which the researcher refined and defined the themes and possible sub-themes within the data set before linking them to the sub-research questions. Thematic analysis was repeated to ensure that the identification of themes and sub-themes was thoroughly done (Maguire & Delahunt 2017; Agostino et al. 2013). The researcher provided the names of themes and distinct working definitions to capture the essence of each theme succinctly and effectively. Clarke and Braun (2013) regard this step as essential in which themes produce a unified story of the data.

*Reporting findings* is the last step of the thematic analysis framework (Braun & Clarke 2006, 2014). For this study, the themes and sub-themes were used to develop a questionnaire to be used in the QUAN phase. An integrated report was produced after analysing QUAN data. The report

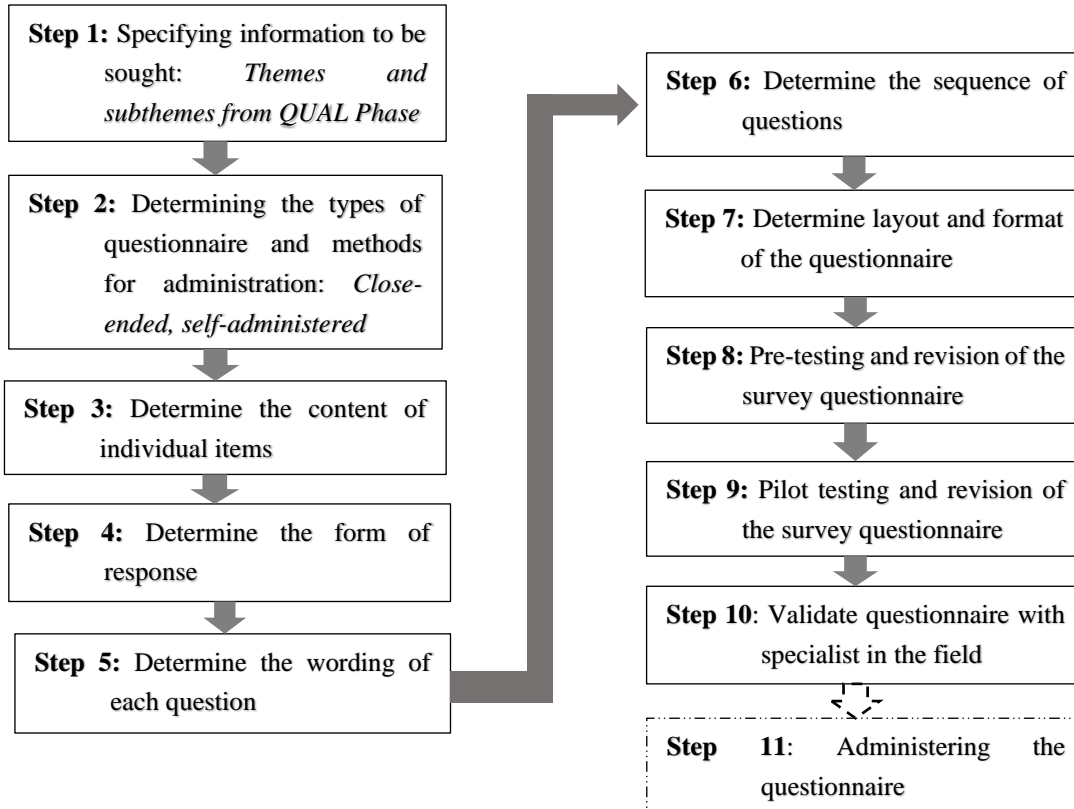
included the use of clear and convincing extracts to support the themes and answer research questions. The interpretation is presented in Chapter 4. The findings from the combined phase are be discussed separately in Chapter 5.

iv. **Quantitative Phase: Instrument development and pilot-testing**

The questionnaire was developed from the findings of the QUAL phase, based on themes and sub-themes. This was based on Creswell (2013) and Creswell and Plano-Clark (2019) who argue that a researcher has an option to use findings of the qualitative phase, such as themes and sub-themes, as variables during instrument development in an exploratory sequential mixed-method design. Themes formed the broad sections of investigations and sub-themes the variables to be measured during the survey. The questionnaire consisted of six sections, the demographic section; factors influencing the adoption of Cloud BI; knowledge of security evaluation; strategies used in the evaluation of Cloud BI; challenges faced in the evaluation process; and the opinions on the components of the security evaluation framework. Churchill (1979) proposes a paradigm for developing a questionnaire that involves several steps. Zefeiti and Mohamad (2015) developed a questionnaire by customising Churchill's model. The model outlines the essential steps that a researcher can follow when designing a questionnaire. This study adapted Zefeiti and Mohamad (2015)'s steps in a questionnaire design by merging and removing redundant steps. A content validation step was included in the questionnaire design. Figure 3.9 shows the steps followed in developing the questionnaire from the findings of the QUAL phase.

By following steps 1 to 6, the questionnaire was produced, and the next crucial steps were completed. The questionnaire was pretested with three local SME decision-makers to check for errors, grammar, repetition of items, the layout of content, and the difficulty of questions. The questionnaire was edited by removing, rephrasing, and repositioning some items based on the feedback from the pre-test. The second draft of the questionnaire was pilot studied with four SME owners who were using ITs to manage businesses, and three IT security specialists (a senior Computer Science lecturer specialising in IT security from a local university; and two IT security specialists from local commercial banks). Further changes were made on recommendation by the IT security specialists. The content validation was done by three security specialists, one from an established IT security company in South Africa and two IT lecturers from one of the local

universities. A statistician was asked to review the questionnaire to look at the scales and measurements used. The validators were satisfied with the content, items and constructs being measured.



**Figure 3.9: The steps in developing a questionnaire**  
Adapted from Zefeiti and Mohamad (2015) for this study

The questionnaire had the following sections:

- Section 1: Demographic information of respondents and SMEs
- Section 2: Factors influencing the adoption and use of Cloud BI by SMEs
- Section 3: Strategies used in evaluating Cloud BI by decision-makers
- Section 4: Challenges faced by decision-makers with the evaluation of Cloud BI
- Section 5: Main aspects considered in proposing a security evaluation framework

The final questionnaire is *in Appendix F*.

### **3.2.7.2. Data collection in quantitative phase using survey questionnaire method**

Quantitative data were collected by both postal and online self-administered questionnaires. Seventy (70) postal and 35 online questionnaires were distributed to SME decision-makers in five towns, namely, Louis Trichardt, Thohoyandou, Mokopane, Musina and Giyani. Decision-makers were requested to complete an informed consent form before completing the survey questionnaire. A total of 45 completed postal and 15 online questionnaires were received. Five postal questionnaires were rejected due to non-completion of critical sections and duplicate submissions, leaving the researcher with 55 questionnaires. Follow-ups were made resulting in two more completed postal questionnaires being received. The final total of valid questionnaires was 57.

### **3.2.7.3. Quantitative data analysis for the qualitative phase**

Data from the questionnaires was captured into an Excel worksheet for verification, cleansing, and coding. The data was then imported into Statistical Package for Social Scientist (SPSS) Version 26 for quantitative analysis with the aid of a statistician. Results were presented in simple frequency tables, graphs, and descriptive statistics. The findings of the QUAL phase and results of the QUAN phase were integrated during interpretation done under SRQs.

### **3.2.8. Credibility and trustworthiness in qualitative data**

Qualitative research designs abide by principles of validity and reliability that are different from those of quantitative design (Cohen et al. 2018). Qualitative designs use terms such as quality, rigour, plausibility, credibility, and trustworthiness to describe validity (Golafshani 2003). Credibility (internal validity) means accurate identification and description of the phenomenon by the research study (Yin 2012; Golafshani 2003). Transferability (external validity) refers to the degree to which the results of qualitative research can be generalised or transferred to other contexts or settings that may be problematic (Marshall & Rossman 2014). Research transferability is enhanced by a thorough description of the research context and the assumptions that are central to the research (Cameron 2015; Marshall & Rossman 2014). Credibility was attained through the honesty, depth, richness, and scope of the data collected, the participants approached, and the extent of objectivity of the researcher (Cohen et al. 2018). In the qualitative phase of this study, credibility depended on the purpose of the participants and the appropriateness of the data collection methods used to capture the purposes (Kikawa 2019; Schoonenboom & Johnson 2017).

The researcher was able to apply both trustworthiness and credibility in the QUAL phase of the study as demanded by the mixed method design being applied.

### **3.2.9. Validity and reliability of a questionnaire**

Validity and reliability have different meanings in qualitative and quantitative designs (Crocker 2015; Golafshani 2003). In quantitative design, validity is based on the premises of positivism and positivist principles, such as controllability, replicability, and predictability (Cohen et al. 2018). Validity refers to the degree to which a research study measures what it intends to measure, while reliability is concerned with the accuracy and precision of what is being measured by the research study (Golafshani 2003). To ensure the validity and reliability of the questionnaire at the design stage, Youssef and Alageel (2012) encourage researchers to reduce or avoid any potential common method variance (CMV), which can be a source of bias in quantitative surveys. The ex-ante and ex-post are two common strategies used to avoid CMV biases in surveys (Podsakoff, MacKenzie, Lee & Podsakoff 2003). According to Podsakoff et al. (2003), the researcher can avoid or minimise potential CMV biases by collecting measures for different constructs from QUAL interview findings and mix the ordering structure of the questions to reduce the likelihood of bias towards the theory-in-use (Podsakoff et al. 2003). The researcher used pre-tests to reduce bias during the questionnaire design in which mistakes were removed. The questionnaire was administered to the respondents by postal and online and this reduced the influence of the researcher on respondents. Furthermore, the CMV was reduced by assuring respondents of anonymity and confidentiality of the study and asked respondents to answer questions as candidly as possible (Chang, van Witteloostuijn & Eden 2010). Content validity was ensured with the assistance of an IT lecturer in the Department of Computer Science at the University of Venda and IT personnel specialising in cybersecurity.

The online questionnaire items were validated to prevent both the submission of incomplete questionnaires and respondents from multiple submissions. The overall reliability of the survey questionnaire was determined using the SPSS application and Cronbach's alpha is reported in Chapter 4.

### **3.2.10. Ethical consideration**

Data collection for this study involved human beings as subjects, therefore the need to address ethical issues throughout (Cameron 2015; Babbie 2014). Several ethical issues were considered as specified in the University of South Africa Ethics Clearance Letter in *Appendices A and B*. Each of the ethical issues considered is briefly described in subsequent subsections. Furthermore, the researchers adhered to the citation requirements of publications work, accurate reporting of results and research findings. Permission to conduct a research study with different subjects in selected SMEs was sought beforehand and confirmed during the data collection exercise. The participants in this research study were adults from sampled SMEs and their consent was sought before data collection.

*Informed consent:* To cater for informed consent, the researcher:

- explained the purpose of the study and the role of each participant.
- requested participants show consent to participate in the study by signing the consent form;

*Right to privacy:* The participants and respondents were guaranteed privacy to information regarding their identity and responses to the questionnaires and interview. All responses were kept in a locker and softcopies were password protected.

*Deception of respondents:* The researcher assured the participants in writing and verbally that the research study was genuine and was not deceived in participating.

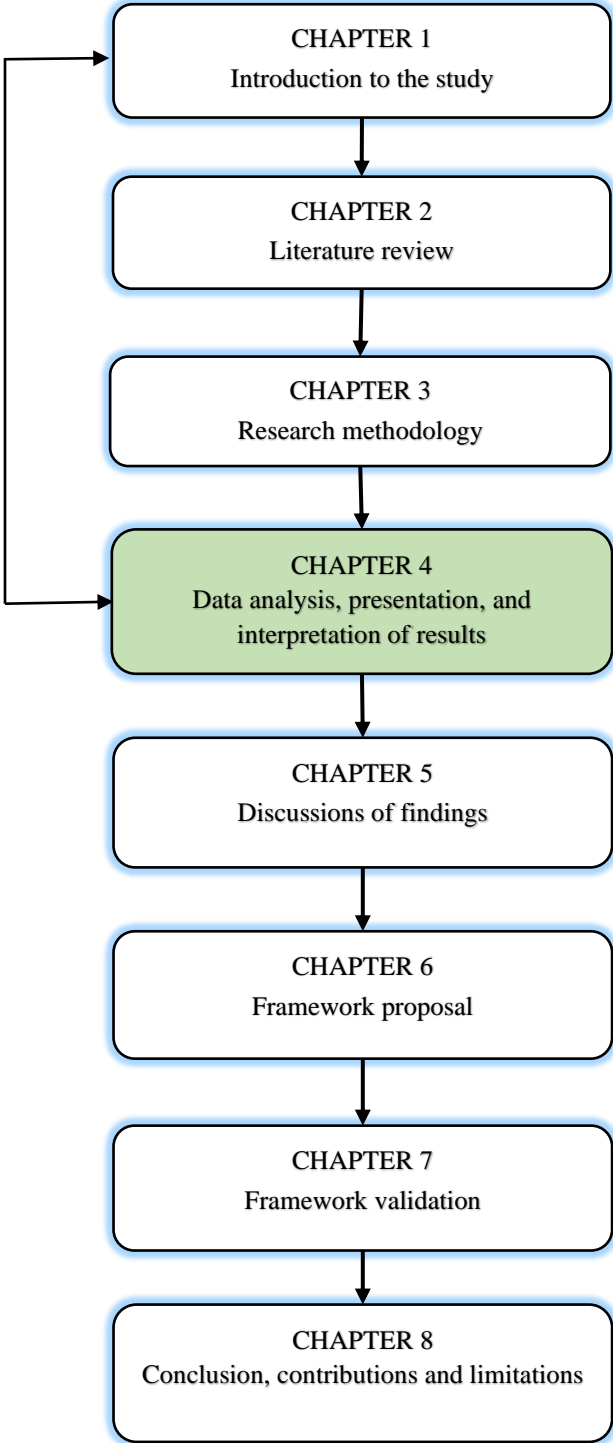
*Right to protection from discomfort and harm:* During the interview sessions, respondents were made to feel comfortable by choosing places and times they wanted the interviews to be held. Questions asked were all neutral and required answers of a general nature.

*Voluntary participation:* Respondents and participants were asked to indicate that they were not coerced to participate in the research study but did so voluntarily. Respondents and participants were free to withdraw from the study without explanation.

### **3.2. Conclusion**

This chapter presented the research methodology and design used in this research study. The chapter showed the research process to be followed and briefly discussed each identified aspect of the process. The empirical study adopted an exploratory mixed-methods design in which data was collected from the decision-makers and then analysed to determine the requirements of the SMEs for the security framework they needed to evaluate Cloud BI. The findings of the QUAL phase and the results of the QUAN phase were integrated at the interpretation stage of the study. The findings were used in proposing the security evaluation framework. The next chapter presents and interprets the results of the study.

**CHAPTER 4 DATA ANALYSIS, INTERPRETATION AND FINDINGS**





## **4.1. Introduction**

Chapter 3 presented the research methodology and design, data collection and analysis methods and research instruments used in this study. The purpose of this chapter is to present and interpret the findings of the QUAL phase and the results of the QUAN phase. The findings from the QUAL phase were presented as themes and sub-themes, while results from the QUAN phase were presented as frequency tables, graphs, and descriptive statistics. Findings from the QUAL phase were supported by interview extracts and results from the QUAN phase. This approach has been used to integrate the results from the two phases of an exploratory sequential design. The remainder of the chapter is organised into two major sections, namely, the presentation and interpretation of the results and the conclusion to the chapter.

### **4.1.1. Findings from the qualitative phase**

The findings of the QUAL are presented in Table 4.1 and were used to design a survey questionnaire which was used in the QUAN phase of the empirical study. Interpretations for QUAL findings were provided under the respective SRQs, which were substantiated by results from the QUAN phase. The interpretation of these findings was jointly done with results of the QUAN phase, as recommended by Creswell (2013) and (Creswell & Creswell 2018).

The results for a reliability test of variables in each of the sections of the questionnaire were based on Cronbach's alpha coefficient, obtained using SPSS (*see Table AP4.1 in Appendix J*). The reliability test results show that the inclusion of the variables being measured was justifiable for all the key sections as it varied from acceptable (alpha = 0.67) to highly acceptable (alpha = 0.859) (Ursachi, Horodnic & Zait 2015; Hulin, Netemeyer & Cudeck 2001). The overall reliability of the 122 variables measured on a Cronbach Alpha test was 0.863, a further indication of how closely related the variables under investigation was.

**Table 4.1: Themes and sub-themes on adopting and using Cloud BI**

| SRQ   | Themes |  | Sub-themes |  |
|---|--------|--|------------|--|
| <i><b>SRQ1:</b> What factors influence the adoption and use of Cloud BI among SMEs in small South African towns?</i>  | 1.     | Benefits of using Cloud BI to support business operations                                  | 1.1.       | The effort made by decision-makers in adopting and using Cloud BI  |
|   |        |  | 1.2.       | Description of the benefits of using various cloud services by participants                                  |
|   | 2.     | Challenges of using Cloud BI to support business operations                                | 2.1.       | Description of the challenges being faced by decision-makers in their effort to adopt and use Cloud BI       |
|   |        |  | 2.2.       | Description of effects of challenges on decision-makers' effort to adopt and use Cloud BI                    |
| <i><b>SRQ2:</b> How do small and medium enterprise decision-makers evaluate Cloud BI before adoption?</i>   | 3.     | Security evaluation strategies and tools for Cloud BI                                      | 3.1.       | Description of strategies in evaluating Cloud BI by decision-makers  |
|   |        |  | 3.2.       | Description of tools used for evaluating Cloud BI by decision-makers of SMEs                                 |
|   |        |  | 3.3.       | The importance of decision-makers understanding security evaluation  |
|   |        |  | 3.4.       | Effects of limited understanding of the evaluation process on the adoption and use of Cloud BI               |
|   |        |  | 3.5.       | Suggestions on security considerations during the evaluation of Cloud BI                                     |
| <i><b>SRQ3:</b> What challenges do small and medium enterprise decision-makers face when evaluating Cloud BI?</i>   | 4      | Challenges faced during the evaluation of Cloud BI   | 4.1.       | Limited knowledge and skills of decision-makers to evaluate Cloud BI   |
|   |        |  | 4.2.       | Ignorance or lack of suitable tools for use by small and medium enterprises in evaluating cloud applications |
|   |        |  | 4.3.       | Challenges of getting relevant information about the Cloud BI from the CSPs and vendors                      |
| <i><b>SRQ4:</b> What do decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises?</i> | 5.     | Knowledge of methodologies, models, and frameworks used in evaluating security in Cloud BI | 5.1.       | Suggestions on the components of a security framework for evaluating Cloud BI by SMEs                        |
|   |        |  | 5.2.       | Opinions and views on the uses of the security framework   |
|   |        |  | 5.3.       | Opinions on type of security framework   |

#### 4.1.2. Demographic information for the study

This subsection presented, analysed, and interpreted demographic information of SMEs and participants for both the QUAL and QUAN phases. A joint display of the demographic results is shown in **Table 4.2**.

**Table 4.2: Demographic information of SME decision-makers**

| Item  | QUAL PHASE (n = 13) | QUAN PHASE (n = 57) |
|---|---------------------|---------------------|
| <b>Number of respondents by town</b>                                  |                     |                     |
| Town A (Thohoyandou)  | 4                   | 22 (38.6%)          |
| Town B (Louis Trichardt)  | 3                   | 14 (24.6%)          |
| Town C (Mokopane)   | 2                   | 10 (17.5%)          |
| Town D (Musina)   | 2                   | 7 (12.3%)           |
| Town E (Giyani)   | 2                   | 4 (7.0%)            |
| <b>Decision-maker</b>   |                     |                     |
| Owners  | 9                   | 36 (63.23%)         |
| Managers  | 4                   | 21 (36.8%)          |
| <b>State of information technology facility</b>                       |                     |                     |
| Good  | 5                   | 19 (33.3%)          |
| Fairly good   | 7                   | 33 (57.9%)          |
| Bad   | 1                   | 5 (8.8%)            |
| <b>Gender</b>   |                     |                     |
| Female  | 2                   | 18 (31.6%)          |
| Male  | 11                  | 39 (68.4%)          |
| <b>Age ranges of decision-makers (years)</b>                          |                     |                     |
| 30 to 40  | 2                   | 13 (22.8%)          |
| 41 to 50  | 8                   | 37 (65.0%)          |
| above 50  | 3                   | 7 (12.2%)           |
| <b>Highest Educational Qualification</b>                              |                     |                     |
| Matric  | 3                   | 7 (7.0%)            |
| Diploma   | 8                   | 42 (73.7%)          |
| Degree  | 2                   | 11 (19.3%)          |
| <b>Experience in using ITs to support business operations (years)</b> |                     |                     |
| 1 to 3  | 2                   | 10 (17.5%)          |
| 4 to 6  | 7                   | 38 (66.7%)          |
| more than 6   | 4                   | 9 (15.8%)           |
| <b>Enterprise innovation adoption style</b>                           |                     |                     |
| Early adopters  | 1                   | 5 (8.8%)            |
| Early majority  | 2                   | 15 (26.3%)          |
| Late majority   | 8                   | 29 (50.9%)          |
| Laggards  | 2                   | 8 (14.0%)           |
| <b>Preferred Cloud BI deployment model</b>                            |                     |                     |
| Secure web access   | 7                   | 33 (57.9%)          |
| Internet access   | 2                   | 17 (29.8%)          |
| Both Web & Internet   | 3                   | 7 (12.3%)           |

The results show that close to 40% of respondents were from Town A (Thohoyandou) with 38.6%, and the least from Town E (Giyani), 7%. These results confirm that SMEs from some small towns use online IT systems to support business management more than those from other towns. In both samples, most of the decision-makers were owners (9 out of 13 participants for QUAL and 63% for QUAN). The results illustrate that the state of IT facilities used to support SME business operations was fairly good by 57.9% and good by 33.3% of respondents. The results further show that there were fewer female decision-makers (31.6%), in SMEs than their male counterparts, (68.4%). Most of the respondents, 65.0%, were agreed between 41 and 50 years. Most respondents (73.7% ) indicated a diploma as the highest academic qualification. The majority 66.7% of the respondents indicated having been using ITs to support businesses for more than 4 years. The majority of the respondents, 50.9%, considered their enterprises to be late majority adopters of IT systems while 26.3% indicated early majority. The findings show that the owners/managers of SMEs were individuals in the economically active age group with a good educational level and were able to use IT systems to support business operations. This further shows that both samples were appropriate in providing the information needed for this study. Most of the respondents, 33 (57.9%), indicated that they preferred to access Cloud BI over a secured web as they could not afford a private connection through the Internet. The results confirm that security was considered very important when Cloud BI was accessed over the web.

The SMEs were categorised based on the number of employees as shown in Figure 4.1.



**Figure 4.1: Distribution of respondents by the number of employees in SMEs**

The results show that most of the respondents, 59.5%, indicated that they employed between 10 and 30 employees, followed by 22.8% employing 31 to 50 employees. Most of the respondents, 82.4% were small enterprise decision-makers while 16.6% were from medium enterprises.

**4.1.3. SRQ1: What factors influence the adoption and use of cloud business intelligence among small and medium enterprises in small South African towns?**

To understand the factors influencing the adoption and use of Cloud BI by SMEs in selected towns of Limpopo, Themes 1 and 2, as well as their sub-themes, were interpreted and supported by selected extracts from participants and descriptive results from the QUAN phase.

**4.1.3.1. Theme 1: Knowledge of benefits of adopting and using Cloud BI**

Findings in Theme 1 indicate that SME decision-makers were aware of the benefits of Cloud BI and were willing to adopt and use the technology (Sub-theme 1.1) provided it was safe and economically viable. The participants described the effort made in adopting and using various online IT systems and Cloud BI (Sub-theme 1.2).

**Sub-theme 1.1. The effort made by decision-makers in adopting and using Cloud BI**

The participants expressed that in the process of adopting Cloud BI. Activities described by participants showed that SMEs were at different stages of adoption of Cloud BI and that meaningful usage of the technology was still very low. In the QUAN phase respondents indicated the stages of adoption of Cloud BI similar to those in the QUAL phase and were consistent with Ettlie (1980)'s MSAM, primary awareness, interest, evaluation, testing and commitment stages. Results for QUAL and QUAN phases are in Table 4.3.

**Table 4.3: Stages of adoption of Cloud BI for 13 participants**

| Variable  | QUAL (n =13)         | QUAN (n = 57)     |
|---|----------------------|-------------------|
|   | f (Participants)     | Respondents f (%) |
| <b>Stage of innovation adoption</b>                 |                      |                   |
| Awareness   | 3 (7, 8 & 13)        | 11 (19.3)         |
| Interest  | 2 (9 & 12)           | 23 (40.4)         |
| Evaluation  | 4 (1, 3, 4 & 5)      | 16 (28.1)         |
| Testing   | 2 (2 & 11)           | 5 (8.8)           |
| Commitment  | 2 (6 & 10)           | 2 (3.5)           |
| <b>Stage of adoption regarded as most difficult</b> |                      |                   |
| Awareness   | 2 (7 & 13)           | 3 (5.3)           |
| Interest  | 2 (8 & 12)           | 8 (14.0)          |
| Evaluation  | 6 (1, 2, 3, 4, 5, 9) | 28 (49.1)         |
| Testing   | 2 (6 & 11)           | 14 (24.6)         |
| Commitment  | 1 (10)               | 4 (7.0)           |

*i. Awareness stage*

The extracts from Participants 7, 8 and 13 confirm that some SMEs were at the awareness stage of adopting Cloud BI, in which gathering information about cloud technology, benefits and possible setbacks were key indicators. Participants expressed willingness to adopt and use the technology in the future if there was a need and subject to approval by colleagues:

I am aware of business intelligence in the cloud because I have attended some workshops on emerging technologies and cloud services, such as cloud business intelligence which were also exhibited... but I think the enterprise can manage with what is there in terms of data management and decision-making. Maybe in the future, I may consult my staff and consider adopting it only if it improves profits. **[Participant 7]**

I am aware of cloud computing although I am not knowledgeable about how the technology works. I have been using online backup facilities like DropBox, OneDrive and Google drive. I have heard about cloud business intelligence, and it did not ring into my head whether to adopt it or not. **[Participant 8]**

Cloud technology is not something new to me because I am familiar with OneDrive and Google Drive on my smartphones which I use to save most of my data on the cloud, but for cloud business intelligence, I only hear people talking about it. I have not yet put much thought into it. I think I will now have a closer look at the technology. I hope it is a better technology than conventional applications. **[Participant 13]**

*ii. Interest stage*

Only two participants indicated that to be at the interest stage of adoption of Cloud BI.

Deciding to adopt technology is a very crucial step in a small business like this one. I had time to look at several online services offered over the cloud. It was so fascinating to realise how much there is on the internet or the web in terms of cloud services. There are so many businesses intelligence I came across and tempting to adopt if one is not careful. I am always interested in using online apps but only how to go around, particularly the new ones in the cloud. **[Participant 9]**

I have been wondering how my friend was doing things so simply and whenever I asked questions, he always has answers. One day he demonstrated a few cloud technologies which he used to process data for his businesses. He does it on his tablet over the net. I am learning something, but I need to put my house in order first, especially my data which is still on hard copies. **[Participant 12]**

*iii. Evaluation stage*

Participants 1, 4 and 5's attestations indicated that they were at the evaluation stage of Cloud BI adoption:

I have signed up for several trial products, some free and others requiring small payments. I was surprised to find a lot of these products on the web. I tried a few solutions including Grow BI Dashboard, Power BI, Databox, SharePoint and BuzzBoard. It is always hard to examine all of them objectively and come to the right choice, particularly if you do not know what you are looking for in the software. To me, they seem to be the same, except for the interface. **[Participant 1]**

I am looking at several free cloud business intelligence apps to see if I can learn something before adopting one. It is a very slow process that requires caution to avoid bad decisions. I cannot assure you of doing the right thing. **[Participant 4]**

By the way, we are not very far from adopting cloud business intelligence. Once we find the right app, we will carefully move the data to the cloud system. But for now, we only use limited resources on the cloud for storage purposes. **[Participant 5]**

These narrations indicate that many evaluation activities were being conducted by SMEs and caution was being taken to avoid adopting the wrong solutions.

*iv. Testing stage*

Attestations by participants 2 and 11 suggest that they were conducting some tests or trials with Cloud BI:

I have tried a few free and trial products on the net but with little success due to several challenges, I need to overcome. As it is, I double up as a manager and IT person and am so busy finding out the best solutions. I am anxious to see something materialising soon and be the first to use the technology around this place. I was amused by the one I tried recently. **[Participant 2]**

My experience with online applications is very good. I have a good background in IT, and I do a lot of evaluations of new solutions, particularly trial versions. I have the challenge of not finishing the testing because of other commitments and only remembering when the trial period has expired. In some cases, I realise that the solution is not as good as it is reported. In one situation, I failed to upload data from Excel to the database of the cloud solution as it kept on freezing. **[Participant 11]**

*v. Commitment / implementation stage*

Only two participants, 6 and 10 perceived their enterprises as being at the commitment stage.

**Participant 6** expressed a view of having decided to commit to Cloud BI but stopped:

At times, I used cloud business intelligence for basic processes such as analysis and displaying trends on graphical displays. Nothing much interesting because I was not able to utilise the facility although. It demanded most of my time and I was afraid of making mistakes that would put the enterprise at risk.

**Participant 10** viewed commitment to Cloud BI as a very difficult challenge, particularly when the data was about to be migrated to the cloud. Uncertainties about security in the clouds became real and forced decision-makers to continue weighing the possibilities of losing business due to cybersecurity risks, such as loss of confidentiality and availability.

On the one hand, I am overwhelmed with this new experience of having broken the barrier in technology adoption and on the other hand the fear of losing all data and information in the cloud. Security assurance becomes a pressing issue even if one has put lots of thinking before adoption. But I enjoy the challenges as they make me realise increasingly about cloud technology.

The findings in the QUAL phase were supported by results from the QUAN phase, (*see Table 4.3 above*), which indicated a fair distribution of respondents among the first three stages of technology adoption: 3 (5.3%) indicated being at the awareness stage, 8 (14.0%) at the interest

stage, and 28 (49.1%) at the evaluation stage. Very few respondents indicated being at the testing, 14 (24.6%), and commitment, 4 (7.0%), stages, respectively.

These findings show that very few SMEs proceed beyond the evaluation and testing stages in the adoption of Cloud BI. This confirms that the evaluation stage is the most difficult for decision-makers to conduct and to make concrete decisions, leading to the successful selection of a particular solution. Results from the QUAL (6 of 13 participants) and QUAN (nearly 50% of the respondents) further confirm that the evaluation stage was perceived as the most difficult stage of the adoption process. It can be inferred that more effort should be put into the evaluation of the Cloud BI in the adoption process.

### **Sub-theme 1.2: Description of the benefits of using various cloud services by participants**

Participants expressed a willingness to adopt Cloud BI because they believed they were beneficial to their enterprises, particularly in data management and decision-making.

#### *i. The importance of Cloud BI for decision-making in SMEs and the need to adopt and use the technology*

Participants perceived emerging self-service technologies, such as Cloud BI, as being important for easy data management to aid the decision-making process in SMEs and to survive economic challenges which require the use of an IT system. The extracts from participants 1, 2, 4, 9, and 10 reveal that decision-makers appreciated the importance of Cloud BI use by SMEs.

**Participant 1** expressed the capability of Cloud BI in solving infrastructure and software problems common among SMEs but said that security challenges presented several obstacles.

Under normal situations, the cloud is the right answer to business IT problems because it can solve our challenges of infrastructure and software we could purchase at high prices. As small businesses, we face many challenges when we want to expand our IT infrastructure and so we intend to move to the cloud at any time when we are satisfied that we can deal with security issues.

**Participant 2** viewed Cloud BI as being capable of solving data management challenges faced by many SMEs.

I like the idea of cloud business intelligence as this can go a long way in assisting me in data processing and decision-making. I have heard a lot about the capabilities of these technologies.



The importance of adopting and using Cloud BI by SMEs was emphasised further by **Participant 4** who said,

To begin with, I acknowledge that cloud business intelligence is very important ... it is difficult to talk about IT without the cloud these days. It is the wish of an ambitious businessperson to use modern technology which most people are familiar with, ... it is regrettable to be behind time. As far as it concerns this enterprise, I know of cloud business intelligence and other cloud services capable of making changes to our fortunes.

**Participant 9** said,

I appreciate the benefits that an organisation like ours can get from cloud business intelligence, particularly cost-effectiveness and reduction in infrastructure.

**Participant 10** elaborated on the benefits of using Cloud BI by SMEs,

Since I started using some form of business intelligence, I have found it easy to collect, store and process data. I think the mistakes I have been making in decision-making have been reduced considerably. Before I relied on my experience...I can say rather instincts at some point. I am now able to access all my data and process them easily over the cloud although I am still sceptical of the technology.

These findings demonstrated that the benefits of Cloud BI and other cloud services have permeated SMEs and reflects on the good experiences and feelings of decision-makers in some of the enterprises.

*ii. Enthusiasm and willingness to adopt and use safe cloud business intelligence among SMEs*

Participants expressed interest and willingness to adopt and use safe and secured Cloud BI in their enterprises.

I am excited when I use new technology, I can tell you that many things are going on around here concerning cloud technology stuff and we have so many cloud service options to consider, not only business intelligence. I am convinced that the cloud has benefits as well as problems related to security because no one has control over the web and what goes on, good or bad. **[Participant 1]**

This was supported by **Participant 9**:

I am ready to use any simple technology. Previously, I struggled to use cloud services... I just need some time to learn and understand how they work before selecting one. I think in time I will join others in the use of cloud business intelligence apps to improve the running of the business. I need more time to search and choose the right product which is stable and safe to use.

These extracts confirm the eagerness of decision-makers to adopt Cloud BI after understanding more about the technology, however, Participant 9 thought that learning the technology was difficult. These findings were supported by the results from the QUAN phase presented in Table 4.4. The results show that the majority of the respondents, 40 (70.2%), indicated having good and very good knowledge of the benefits of Cloud BI. For the duration of awareness of Cloud BI, 24

(42.1%) respondents had been aware of Cloud BI from 1 to 3 years and 17 (29.8%), 4 to 6 years. Most of the respondents, 49 (86.0%) rated their knowledge of the benefits of using Cloud BI as good and very good. The results confirm that decision-makers got information about Cloud BI and other cloud services from various sources such as the web, friends, e-mail adverts, and employees. The main source of information was the web, as indicated by 29 (50.9%) of the respondents and employees were indicated as the smallest source, 3 (5.3%). It can be inferred that decision-makers were familiar with Cloud BI and its benefits to improve the business operations of SMEs.

**Table 4.4: Knowledge of benefits of the use of Cloud BI among SMEs**

| Variable   | n =57         |           |
|--|---------------|-----------|
|  | Responses     | f (%)     |
| Knowledge of Cloud BI                            | Bad           | 12 (21.1) |
|  | Good          | 40 (70.2) |
|  | Very good     | 5 (8.8)   |
|  | <b>Total</b>  | 57 (100)  |
| Duration of awareness of Cloud BI                | < 1           | 9 (15.8)  |
|  | 1 to 3        | 24 (42.1) |
|  | 4 to 6        | 17 (29.8) |
|  | > 6           | 7 (12.3)  |
|  | <b>Total</b>  | 57 (100)  |
| Knowledge about the benefits of Cloud BI in SMEs | Very good     | 14 (24.6) |
|  | Good          | 35 (61.4) |
|  | Bad           | 7 (12.3)  |
|  | Not sure      | 1 (1.8)   |
|  | <b>Total</b>  | 57 (100)  |
| Source of information about Cloud BI             | Research      | 29 (50.9) |
|  | Friends       | 17 (29.8) |
|  | E-mail Advert | 8 (14.0)  |
|  | Employee      | 3 (5.3)   |

Respondents were asked to indicate on a 3-point Likert scale (more likely = 3, not sure = 2 and less likely =1) the extent to which the benefits of Cloud BI were influencing decision-makers to recommend that their enterprises adopt the technology.

**Table 4.5: Influence of benefits on the recommendation to adopt Cloud BI**

| Benefit                                     | Ratings of benefits (n =57) |                   |                      |      |     |
|---|-----------------------------|-------------------|----------------------|------|-----|
|   | More likely<br>f (%)        | Not sure<br>f (%) | Less likely<br>f (%) | Mean | SD  |
| Improving decision making                   | 52 (91.3)                   | 2 (3.6)           | 3 (5.3)              | 2.9  | 0.5 |
| Reduced overhead costs of BI applications   | 51 (89.5)                   | 4 (7.0)           | 2 (3.5)              | 2.9  | 0.4 |
| Improving competitiveness                   | 51 (89.5)                   | 3 (5.3)           | 2 (3.6)              | 2.8  | 0.5 |
| Affordability of cloud services             | 50 (87.7)                   | 4(7.0)            | 3 (5.3)              | 2.8  | 0.5 |
| Data analysis, visualisation, and reporting | 50 (87.8)                   | 4 (7.1)           | 3 (5.3)              | 2.8  | 0.6 |
| Improving customer care                     | 48 (84.3)                   | 6 (10.6)          | 3 (5.3)              | 2.7  | 0.6 |
| Improving data management                   | 46 (80.8)                   | 8 (14.1)          | 3 (5.3)              | 2.6  | 0.7 |
| Professionalism in information analysis     | 46 (80.8)                   | 9 (15.8)          | 2 (3.6)              | 2.8  | 0.5 |
| Easy integration with existing technology   | 45 (79.0)                   | 7 (12.3)          | 5 (8.8)              | 2.8  | 0.4 |
| Rapid deployment and implementation         | 43 (75.4)                   | 11 (19.3)         | 3 (5.3)              | 2.7  | 0.6 |
| Simplicity of Cloud BI                      | 43 (75.4)                   | 9 (15.8)          | 5 (8.8)              | 2.7  | 0.6 |
| Elasticity of Cloud BI                      | 42 (73.7)                   | 12 (21.1)         | 2 (3.5)              | 2.7  | 0.6 |
| On-demand availability of Cloud BI          | 40 (70.2)                   | 14 (24.6)         | 3 (5.3)              | 2.6  | 0.6 |
| Security of the cloud                       | 35 (61.4)                   | 8 (14)            | 14 (24.6)            | 2.7  | 0.6 |

The results displayed in Table 4.5 show the ratings, mean scores, and standard deviations. The majority of the respondents (61% to 92.5%), with mean scores of 2.7 to 2.9, affirmed that decision-makers were more likely to be influenced to recommend the adoption and use of Cloud BI by all factors listed in Table 4.5. The factors highly rated as more likely to influence the adoption of Cloud BI were: improving decision making (91.3%); the reduced overhead of Cloud BI (89.5%); improving competitiveness (89.5%); affordability of cloud services and data analysis, visualisation, and reporting (87.7%). However, on-demand availability of Cloud BI was rated low by 40 (70.2%) respondents, mean score 2.6 (SD = 0.6), and security of the cloud environment by 35 (61.4%) respondents, mean 2.4 (SD = 0.9). The findings show that decision-makers were certain about some benefits of Cloud BI but unsure of how secure the clouds were. The main influential factors were those related to data management, decision making and the low costs of Cloud BI.

The Chi-Square test of independence,  $\chi^2$  (38.360a;  $df = 6$ ;  $p = 0.000$ ;  $N = 57$ ) shows a significant association between the knowledge about the existence of Cloud BI and the benefit that could be derived from their use by SMEs to improve business operations and decision-making, (*See Table AP4.2 Appendix J*). These results show that the knowledge about Cloud BI played an important role for decision-makers to realise the benefits of Cloud\_BI use and this could encourage them to see ways of evaluating the technology for future adoption and use.

#### **4.1.3.2. Theme 2: Challenges to the adoption and use of Cloud BI to support business operations**

The study found that decision-makers faced many challenges in their effort to adopt and use Cloud BI in their enterprises. The findings from the QUAL phase, Theme 2 and its two sub-themes are presented in this sub-section. Results from the QUAN phase were used to elucidate the QUAL findings.

##### **Sub-theme 2.1: Description of challenges preventing decision-makers from adopting and using Cloud BI**

The expressions by participants were categorised into four major challenges, namely, fear of security breaches in the cloud environment, CSP selection challenges, fear of financial risks due to service disruptions and litigations, limited knowledge of about the types of Cloud BI needed to select the most appropriate application and physical security issues with CSPs in different jurisdictions.

###### *i. Fear of security breaches in the cloud environment*

The QUAL phase found that participants were prevented from adopting Cloud BI due to the fear of potential security breaches by criminals, such as hackers, and other security threats that could exploit vulnerabilities in cloud computing technologies. These were deterrents to SMEs' efforts to adopt and use cloud services. A few excerpts support the stated findings of security breaches and cyber threats held by participants:

We may lose data or processes, particularly when system update activities take place during peak times where one can experience system unavailability, which may be data loss or corruption, particularly in a cloud shared by many users...these web-based applications can change without notice and the service providers and

developers may not be aware of different data formats that users use. Once the formats are changed, then we will have problems with availability. **[Participant 2]**

I think you are aware that we now have more security issues than before due to the use of the Internet, particularly the web. One can't talk about the internet or web without thinking of security breaches that affect data security and privacy, something that small businesses are not prepared to deal with. I think storing data in the cloud has a danger that it affects many threats I'm not aware of. The manager must be careful to surrender data to hackers and other cybercriminals by storing it in the clouds. **[Participant 4]**

We operate in a dangerous environment where either our competitors or even the providers have the potential to steal our data and show it to the public. It is not clear how we can trust the cloud with data without being certain of the security of an application. It is not obvious that our applications will be compatible with cloud platforms or software to be used. There is a potential that we may have to convert our data to other formats before uploading it, the danger of this is a corruption of the data to an unusable format leading to processing failure. **[Participant 5]**

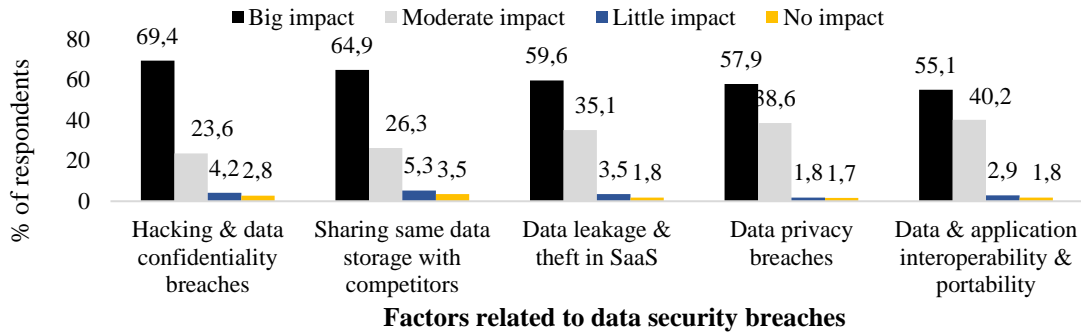
These attestations prove that decision-makers were aware of their obligation of keeping the enterprise data safe and were comfortable with preserving the status quo if their data were to remain secure. Furthermore, the excerpts show that decision-makers were afraid of the consequences posed by unavailable service due to data and applications, incompatibility issues in the event of cloud technology upgrades, changes in format or web apps, and data corruption in the multitenant environments alluded to by all participants. Decision-makers were not able to evaluate these security eventualities in all Cloud BI.

Participants expressed the challenges of ascertaining which Cloud BI was secure and suitable for their business needs. They were worried about the security functionalities of unfamiliar applications and the possibility of having malware in their information systems because of adopting Cloud BI with security flaws. These two attestations confirm the above observations:

One major challenge lies with the security of data, if we place and start processing using cloud solutions, it is difficult to tell which cloud systems are more secure because different providers claim to meet the security requirements and it's difficult to prove that. **[Participant 3]**

My main worry is on the security and functionalities of new apps; I am not familiar with. There are risks associated with adopting these cloud services as they may bring about malware which may cause problems in our computers. Cloud technologies are different from Office Suite we buy and then install, here we are talking about a new technology one has no control over and is not installed onsite. We are not sure how secure the data will be and how to access it. The idea that data is kept on my behalf by someone is tricky and scary. **[Participant 8]**

In the QUAN phase, respondents were asked to rate the impact of data security breaches in influencing the decision to adopt and use Cloud BI on a 4-point Likert scale (4 = big impact, 3 = moderate impact, 2 = little impact and 1 = no impact) *see Figure 4.2.*



**Figure 4.2: Impact of cyber breaches on decisions to adopt Cloud BI**

The results show that factors related to information and data security in the cloud had a moderate to big impact in preventing decision-makers from adopting Cloud BI. The majority of the respondents, 55.1% to 69.4%, were influenced by factors related to data security issues. When deciding to adopt Cloud BI, most of the decision-makers were deterred by hacking and data confidentiality, while fewer were discouraged by data and application compatibilities. These findings confirm that decision-makers faced challenges in evaluating how secure Cloud BI was as they depended much on cloud security information in the public domain.

*ii. Cloud service provider's selection challenge*

Participants were of the view that it was difficult to select CSPs from several available providers offering Cloud BI but using different technologies:

I find it difficult to select a reliable and safe service provider, all the providers I know are commercial and high priced and they provide trials for a short time which I may not be able to finish assessing. Cheap or free solutions cannot be trusted because it is difficult to tell whether the CSPs exist and will continue offering reliable services. **[Participant 5]**

One must be careful with bogus service providers who promise what they cannot provide but end up asking for payment for the service which was initially offered for free. Once you are in, then it becomes difficult to move out. **[Participant 8]**

**Participant 11** raised concerns about the trust of CSP in providing enough security in the cloud.

It is difficult to ascertain whether the CSP uses the correct security controls to protect data as promised.

Other participants expressed that decision-makers were afraid of vendor and data lock-in, a security challenge likely to be experienced when an enterprise decides to switch from one CSP to another. They feared being prevented from migrating data and applications to the new CSP or cloud. Quotes from Participants 3 and 7 confirm this:

I am not sure if it is possible to move from one provider to another without having to face security problems that affect the integrity of data and information. I expect this to be smooth without losing data or being corrupted. **[Participant 3]**

I am afraid of being stuck with one provider, particularly when we fail to move out once we want to use alternative providers. **[Participant 7]**

The two assertions show that decision-makers did not trust the security provision by CSPs and were afraid of being stuck with a certain provider when they decided to leave for another provider.

Decision-makers were afraid of financial risks through payments of hidden costs, and loss of data due to unexpected closure or CSPs going bankrupt. Two participants viewed CSPs not honouring contractual obligations after SMEs had committed to adopt the Cloud BI with a provider as a challenge.

I can have things verified for various critical security issues, however, online apps are a problem in that one can sign a contract only to find that not everything being said by the supplier is provided. Worse still, one may not be able to contact the service provider after entering into a deal and having paid. **[Participant 7]**

Participants alleged that decision-makers were afraid of being manipulated into signing fake contracts that CSPs would later dishonour and demand bigger subscription fees than stipulated after the enterprise has migrated its data and applications to the cloud. The following quotes from participants 3 and 7 support these assertions:

At times, the providers advertise the product as free, but when you subscribe, they charge high prices or just give limited access and services than claimed. No one knows what would happen if the organisation goes completely to the cloud. Losing control of data to CSP while it is safe is a small issue but having data being tampered with or accessed by competitors as they like is not acceptable. **[Participant 3]**

In some cases, CSPs can lure customers pretending that the service is free or cheap only to discover after adopting that it is not for free but more expensive when they demand more money. **[Participant 7]**

The possibility of theft of data and information from the cloud by CSPs and their employees was another factor that led to mistrust of CSPs by decision-makers. Participants pointed out that decision-makers faced the challenge of discriminating genuine CSPs from fake ones and the risk of exposing enterprise data and information to cyber-attacks.

It is problematic to know the nature of the cloud provider and the type of service being given without proper evaluation. I cannot place the safety of my data and business in the hands of strangers I am not sure of. I have heard and read of many negative stories about businesses losing information ... their data being exposed to the public or paid to prevent disclosure of their data to the public by hackers. It is difficult to tell whether the source of the problem is the service providers or the application. **[Participant 1]**

The excerpt shows that decision-makers feared subscribing to malicious CSPs who could hack clients' data, causing security breaches that compromised privacy and trust, consequently affecting

business reputation. Attestations showed that decision-makers feared the unexpected close-down of CSP which could leave the enterprises stranded with data locked in the cloud. Two participants confirmed that decision-makers were worried about the future existence of some CSPs:

We cannot fully trust cloud service providers, suppose the business intelligence just disappears from the web without a trace, then our organisation will be doomed, it will lose all important data and information.  
**[Participant 3]**

What if the person entrusted with the data decides to shut down today without my knowledge...Do you think we will be consulted? I am not sure how we can protect the data and applications we are using if we join the cloud. Although there are many business opportunities in the cloud, we feel it is not yet safe to put most of our stuff there. **[Participant 8]**

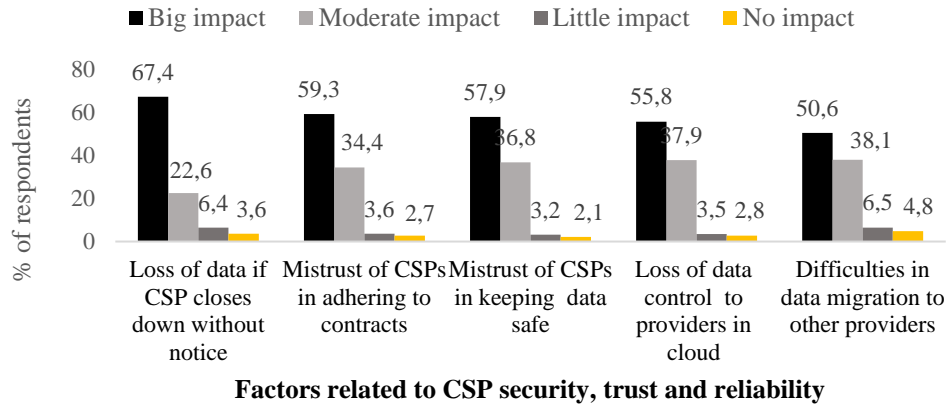
Furthermore, participants expressed that decision-makers perceived loss of data control to CSPs after signing SLAs and migrating to the cloud as a challenge that affected their efforts in the adoption and use of Cloud BI.

I am afraid that I may lose data control when we start using cloud business intelligence. I have no idea how much control of data and information we will have when we decide to use cloud business intelligence. How do I know that I am giving data to an unreliable provider who pretends to be a genuine organisation?  
**[Participant 2].**

Fully adopting cloud applications means that we have fully surrendered our data to strangers who can do what they want with it because we do not have control, we may get stuck in one provider for life. We are not sure if the provider will still be operating in the next few years to come. **[Participant 3]**

QUAN results in Figure 4.3 show that the mistrust of CSPs tended to have a big but negative impact on the effort of decision-makers to recommend their enterprises to adopt Cloud BI. The results show that five factors related to CSPs have overall a moderate to a big impact on influencing decision-makers to decide not to adopt Cloud BI. The majority of the respondents (51% to 67%) indicated that decision-makers mistrusted CSPs for data security, trust control, and service reliability. The results indicated that decision-makers were hesitant to adopt Cloud BI because of the lack of trust in CSPs due to the fear of losing data control once they migrated to the cloud. These findings from both phases seem to concur that decision-makers mistrust CSPs in several crucial areas that affect decision-making when selecting Cloud BI, which require a proper evaluation of each, otherwise this could lead to financial and reputational risks for the enterprise. The respondents indicated that decision-makers feared the consequences of being stuck with a CSP whose survival was uncertain. This could lead to business failure due to poor performance.





**Figure 4.3: Challenges related to CSPs preventing the adoption of Cloud BI**

*iii. Fear of financial risks due to service disruptions and litigations*

Results confirmed that financial risks were identified as the major factor preventing the uptake and use of Cloud BI among SMEs. Findings show that decision-makers feared financial losses that enterprises were likely to suffer when they started using Cloud BI. Financial risks were cited as arising from several sources. **Participant 2's** attestation confirms that when an enterprise loses its data, it will lose revenue and its image will be tarnished:

I am afraid of being a victim of circumstances. Losing data is like losing money and reputation. I am not sure how to react if my data and information were to remain locked into the cloud after the provider removes the website. This will bring disaster by losing all important data ... an organisation's precious asset.

**Participant 3** said that adopting Cloud BI without proper evaluation was unattainable because enterprises could lose revenue by paying for sub-standard solutions:

Financial risks take a different form, particularly with online solutions. You may find paying for a solution that was initially for a free subscription in the guise of getting more functionality. After paying, you find that the app is below what you expected...how would one force the provider to provide the right service.

Attestations by participants 4, 6, and 7 show that decision-makers were of the view that free hosted Cloud BI was used by CSPs to trick interested enterprises into signing contracts which could lead to financial loss:

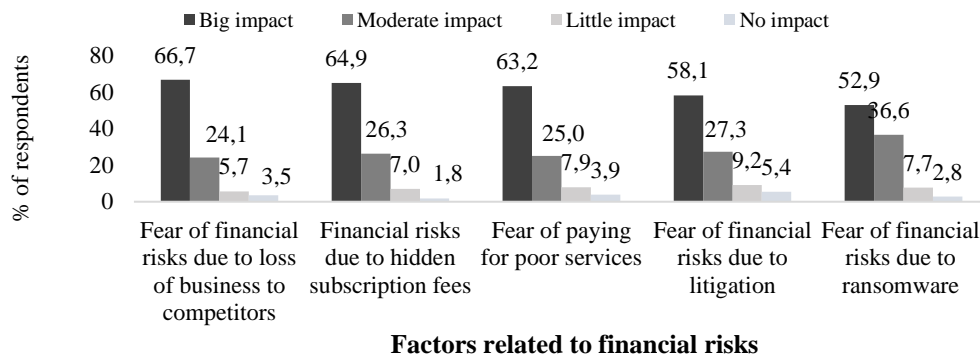
At times, these service providers may front free applications as being free, only to find after successfully adopting, start demanding payment, when they know that your data is already in their control, you will either comply or risk quitting with your vital information remaining in the hands of the service providers. **[Participant 4]**

Another crucial thing to remember is that service providers are in the business of making money and try to lure as many unsuspecting individuals as possible into using their services. At times you subscribe when the service

is free or affordably cheap, then after the service provider has seen that you are now heavily relying on the service, an upgrade demanding subscription and payment suddenly appears. **[Participant 6]**

Hidden costs arising from online services are a financial setback for small businesses because one wants to use something cheap at a stable price. We, small businesses have no extra money for such luxuries which may compromise the fame of the enterprise. What I am saying is that some service providers disguise the service as being free or cheap only for customers to find afterwards that it is not for free or cheap but expensive when they are required to make some additional payment for this and that. **[Participant 7]**

In the QUAN phase, respondents were asked to rate the impact of possible financial risks raised in the QUAL phase and the literature as factors preventing the adoption of Cloud BI by SMEs. Results for ratings of financial risks that were perceived as being deterrent factors on the ability of decision-makers to recommend Cloud BI are depicted in Figure 4.4.



**Figure 4.4: Financial risks due to litigation and loss of services to customers**

The results confirm that the fear of financial risks arising from the use of Cloud BI was an influential deterrent in the adoption of the technology as indicated by the majority of respondents, 52.9% to 66.7%. The fear of financial risks due to loss of business to competitors and fear of financial risks due to hidden subscriptions were indicated as having the most negative impact among decision-makers. The findings show that regardless of the varying impact that each challenge posed, they were crucial in influencing the decision-makers not to recommend SMEs to adopt and use Cloud BI. Respondents indicated that decision-makers were afraid of paying for poor services that could be provided by some CSPs. The inability of decision-makers to evaluate security in Cloud BI and CSPs was a challenge to the adoption of the technology. The findings show that SMEs are particularly averse to IT solutions which may impact SMEs' profitability and survival negatively.

iv. *Limited knowledge of the types of Cloud BI needed to select the most appropriate application*

Participants doubted the abilities of decision-makers in selecting the right application from a host of Cloud BI available, mostly from the websites offered by different CSPs. Selected excerpts support the notion that decision-makers had very little knowledge of the security of Cloud BI and this caused selection challenges.

I will know a lot of these cloud applications with time. For the time being, I am only worried about finding one which is easy to use and can work for us. Without good skills in cloud technology, one is likely to face the problems we are experiencing. It is difficult to select the right application, one has little information about the applications and service provider. I think, with little knowledge in assessing these applications, lady luck should be on your side to get the desired results. **[Participant 6]**

I bet if one can remember all the names of the applications available. It would be sheer luck to bump into the right one if one has little or no idea how to go about selecting applications. The only advantage is that I am getting to know a few things about what one should check in a cloud solution. **[Participant 9]**

I wish things could have been as simple as how the technology is marketed. You realise that you have no idea when you start searching for applications. You come across new things all the time making it difficult to be acquainted with one application. I remember apps like SharePoint, Power B and Excel. **[Participant 10]**

The QUAN results in Table 4.6 support the findings in the QAUL phase on the influence of knowledge and skills in the use of Cloud BI in SMEs. The data was collected by asking respondents to rate on 4-point Likert (big impact = 4 to none =1) how knowledge and skills prevented the adoption of Cloud BI. The mean scores and standard deviations for each item were computed and recorded in Table 4.6. Respondents rated their knowledge and skills in key security aspects of Cloud BI as having a moderate to a big impact, preventing their decision-makers to adopt the technology. All knowledge and skill factors were rated with mean scores of 3.4 to 3.6 and SDs from 0.6 to 0.7. This indicated that respondents regarded knowledge and skills among decision-makers as having a comparably similar impact on the decision made to the adoption of Cloud BI. Limited knowledge about CSPs' reliability and security vulnerabilities in Cloud BI were rated as having a big negative impact by 66.5% and 64.9% of respondents, respectively. On the skills challenge, 59.5% of respondents rated lack of necessary skills to evaluate Cloud BI as having the biggest impact, mean score 3.5 (SD = 0.7) and lack of knowledge of how the cloud works rated low, mean score 3.4, by 50.7% of respondents. The study found that limited knowledge about CSPs reliability, Cloud BI flaws, security about deployment models, deficiency of skills in using

Cloud BI, and evaluating the technology were the main challenges among decision-makers in the selected towns.

**Table 4.6: Impact of knowledge and skills in preventing the adoption of Cloud BI**

| Knowledge and skills challenges related to   | Impact ratings (4 to 1) |           |         |         | Mean | SD  |
|--|-------------------------|-----------|---------|---------|------|-----|
|  | Big                     | Moderate  | Little  | None    |      |     |
| Limited knowledge about the reliability of cloud service providers                     | 38 (66.5)               | 16 (28.1) | 2 (3.6) | 1 (1.8) | 3.6  | 0.7 |
| Limited knowledge about security vulnerabilities in the cloud business intelligence    | 37 (64.9)               | 17 (29.7) | 2 (3.6) | 1 (1.8) | 3.5  | 0.7 |
| Limited knowledge of security in different cloud deployment                            | 34 (59.5)               | 19 (33.3) | 2 (3.6) | 2 (3.6) | 3.5  | 0.7 |
| Limited knowledge about security features of Cloud BI                                  | 29 (50.7)               | 26 (45.7) | 1 (1.8) | 1 (1.8) | 3.5  | 0.6 |
| Limited skills to identify and select the most appropriate cloud business intelligence | 34 (59.5)               | 20 (35.1) | 2 (3.6) | 1 (1.8) | 3.5  | 0.7 |
| Limited knowledge of how the cloud works   | 29 (50.7)               | 24 (42.2) | 3 (5.3) | 1 (1.8) | 3.4  | 0.7 |
| Limited skills in using cloud business intelligence for business purposes              | 33 (57.7)               | 21 (36.9) | 2 (3.6) | 1 (1.8) | 3.5  | 0.7 |

v. *Physical security issues with CSPs in different jurisdictions*

Physical security of infrastructure at the data centres was considered as another factor that influenced the adoption of Cloud BI by SMEs. Some participants' attestations showed that decision-makers were concerned with security at data centres used to store their data.

I do not know what will happen if the computers were stolen or break-down, I lose everything in that cloud and start over. I can tell you that most of the service providers are not local, they quote us in other currencies, they are not South African. **[Participant 1]**

A service offered by a third party is difficult to monitor, especially if one is not able to physically meet the provider. Identifying and deciding which product is safe to adopt can be a problem with self-service apps like cloud business intelligence for our small businesses because we can easily be tricked into accepting anything on offer at that time. **[Participant 7]**

These assertions reveal the traditional view of security rooted among decision-makers, that they should have access to CSPs as well as data centres. They believe and trust what they see. They expect to inspect data centres or have first-hand experience with all technologies before they adopt and use them.

#### **4.1.4. SRQ2: How do decision-makers evaluate Cloud BI before adoption?**

The findings of this research question showed how decision-makers engaged in the security evaluation of Cloud BI. Findings from the QUAL phase, Theme 3 and its sub-themes and results from the QUAN are presented and interpreted in this subsection.

##### **4.1.4.1. Theme 3: Security evaluation strategies and tools for Cloud BI**

The findings presented were on how decision-makers evaluated Cloud BI and the considerations they made during the evaluation process, particularly for security-related issues. Participants described strategies and tools that they could use to evaluate cloud services and the considerations they made. The findings reveal that participants had different constructive views and understanding of the evaluation and how it should be done.

##### **Sub-theme 3.1: Strategies used in evaluating Cloud business intelligence**

The narratives from the participants show what decision-makers regarded as security evaluation for Cloud BI, how it should be conducted and the tools that should be used. The findings show that participants understood security evaluation in Cloud BI as involving:

*i. Assessing authentication, authorisation, and data security in the application*

Participants felt that the use of free trial versions of the services on the web presented them with an opportunity to evaluate Cloud BI before the adoption. The attestations made by participants 5, 6, 8, and 9 show that decision-makers were familiar with the use of trial versions, a common practice encouraged in the IT industry for potential users to familiarise themselves with the solution and whether it meets business needs. Participants believed that the use of trial versions enabled decision-makers to identify flaws in the solutions and possible threats that could compromise data and information security. Some participants suggested checking authentication, authorisation, easy migration, and retrieval of data without corruption, as the basis for the evaluation of the Cloud BI. Therefore, free trial versions of applications became crucial. The following excerpts support the findings:

... the owners need to make sure that the application is secure, and no one can use the app without permission. I focus on how secure it is when logging in and logging out. I need to check if the interface can easily be abused and give the intruder access to the system by bypassing the login process, ... whether the application can log me out automatically. **[Participant 5]**

I will be tactful in my evaluation... I mean doing things one at a time until I am certain that the application is safe for use by the enterprise. You can be patient and compare several cloud business applications checking for the obvious flaws in the interface, data compatibility issues with data retrieval. Before I use online backup storage, I 'googled' and found a lot of information comparing different types of online backup storage, particularly the cloud. **[Participant 6]**

I usually start the evaluation by using free trial versions to see if the application supports or allows easy data transfer from my computer to the cloud and back. I am a person who does not like to put much effort into this which does not work. I want a smooth data transfer between the cloud and my computer...do you understand.... I want to know the security features the system has besides those advertised... I need to check whether the system supports the types of data we work with. **[Participant 8]**

Evaluation means I should verify whether what the service providers say about the technology is true or not.... One does not need to be technically sophisticated to check basic security issues such as passwords, the ability to retrieve data without corrupting it, recovery facilities and functionalities, the interface, I will check if the cloud application integrates smoothly with the existing applications without any technical issues including data upload, it is wise to avoid the difficult solution. **[Participant 9]**

The responses by participants show that some decision-makers had ideas about assessing security features such as interfaces for access control of cloud applications. Decision-makers were convinced that assessing access control was an appropriate strategy for the security evaluation of Cloud BI to determine if unauthorised users were able to access the application.

*ii. Gathering critical information about threats and flaws in the identified cloud business application*

Information about the security aspects of an application was essential for evaluation purposes. This was shown by some participants who suggested the use of free information from different sources to evaluate the application after conducting checks on the trial versions. Participants were aware of different sources of information such as security organisations, websites, IT reports, blogs, friends, open web, and possibly IT specialists. The extracts from the transcripts of participants 1, 2, 3 and 8 highlight the importance of using existing information about security flaws in Cloud BI deployment and the service delivery model in the evaluation process:

I am sure that security organisations rate each popular business IT solution, and I can find this information on the web which makes life easy for laypeople like me. I can find something about the application, who provides it, the advantages and limitations, security breach history where possible. **[Participant 1]**

If I need to adopt a cloud service, I do a lot of research about it, paying attention to its shortfalls regarding data security and portability.... Many solutions have already been evaluated by some experts and information is there on the net and can be useful in evaluating the solution to be adopted, I like the ratings of software in terms of functionality, security, user-friendliness, and cost. I look at the specifications and notable security breaches history if available. **[Participant 2]**

I do take a lot of time reading about IT solutions I am interested in so that I find more about the dark side of it. I am anxious to try several products to get as much information as possible, but time does not allow me. I am always busy with other important tasks within the business. At times, I watch YouTube demos on apps, particularly how to use them. **[Participant 3]**

Having much information about the new system is more important than anything else. Under normal circumstances, I will get such information from friends, the web and maybe from experts. If I find relevant information, I then give myself some time to learn the system before the trial window period expires. I rely on my peers' experiences and at times am fortunate to have subordinates who seem to understand IT security. I discuss my ambitions about cloud services with subordinates who have a passion for IT, products who come and encourage me to try to use Cloud BI. **[Participant 5]**

The finding indicates that decision-makers appreciated the importance of searching for current and historical information about Cloud BI from credible sources such as security organisations, websites, friends who use the system, and IT specialists. These were a desirable understanding by participants because past and current information remain vital in making meaningful decisions in the adoption of any IT solutions.

*iii. Examining the history of a CSP regarding security, reliability, trust and contracts, and business continuity*

Cloud services are offered by third parties, the CSPs, who provide infrastructure, platforms, and software needed by the clients. Participants suggested that decision-makers should examine the CSPs' history in security, reliability of service provision, and trust and contracts, considering the business value of Cloud BI to the enterprise. Selected extracts from interviewees attest to these assertions:

I am eager to verify background checks on a vendor to see which other apps they provide and their performance in protecting data. Security is essential. I can check this from discussion forums on what others are saying about the applications of interest to the enterprise. **[Participant 2]**

Every enterprise seeks to work with a service provider who is flexible and gives more control over upgrades and maintenance so that one can manage them. It is important to check how often the systems are not available and the effect on business. It is pointless to work with a provider whose system is always down. **[Participant 8]**

I need to know how data security in the cloud is catered for. I can use records of previous data breaches, their effects on enterprises, and what the provider did to correct the situation. Where possible, I request information on how the provider implements security when data is stored in the cloud. **[Participant 9]**

Some participants commented that decision-makers verified that they were signing the correct contracts which stipulated what the CSPs were providing, to avoid being tricked into signing

wrong SLAs. Participants pointed out that CSP reliability in providing quality services was very important as emphasised in this excerpt:

I need to check my contractual obligations and what the CSP should do. One should look at how reliable the provider is in providing correct information upon request **[Participant 4]**.

Another participant thought that the time taken to respond to queries and the type of responses given were essential in judging whether the CSPs was reliable and trustworthy, or not.

If a CSP fails to answer my queries within the anticipated time, I abandon the app and look for another one. If the answers given by CSP are not convincing, I leave them and look for something else. There is plenty of cloud business intelligence from which one can get a possibility for the enterprise. I do not spend much time on CSPs who do not co-operate or those who give incomplete and unreliable information about their services. **[Participant 5]**

*iv. Consulting friends who have experience in cloud applications*

Participants regarded their friends and business colleagues as important sources of information for evaluating IT solutions, including cloud services. Participants 7 and 8 expressed their reliance on friends and colleagues whenever they evaluated business solutions.

At times it is wise to be friends ... even colleagues in similar are the best solution to this problem. At times, I can assess various recommended apps before I consult and then make a choice. **[Participant 7]**

I prefer to ask my friends from other enterprises every time there is a problem with new apps I want to use, then I decide from what they say. I compare what my friends say and what I find on the websites of the providers' new technologies whenever I have time. In many cases, information on a new technology gets to us well after some other enterprises have benefited from using it. I visit the websites of other service providers to familiarise myself with their products. **[Participant 8]**

Although the idea of consulting friends and colleagues was good, it cannot be the sole method for evaluating Cloud BI because friends might not be familiar with security issues within the cloud. Friends may recommend a defective application. In the final analysis, decision-makers need to evaluate the applications, one way or the other.

*v. Using existing guidelines and checklists to evaluate security in cloud business intelligence*

Participants suggested the use of existing evaluation tools, such as guidelines and checklists as another strategy for evaluating Cloud BI. However, participants were not certain of which one to use and where to find tools.

I may not be able to do a security evaluation per se, but I should be able to perform a basic evaluation if there are guidelines to assist me. **[Participant 7]**



I will prefer to use guidelines from the web or the documentation that comes with the app when facing challenges. I have not evaluated cloud business intelligence because I use what my friends recommend. At times, it is difficult to find such guidelines which are suitable for small businesses **[Participant 8]**

I guess we should have simple guidelines, checklists, or mechanisms for checking the vulnerabilities and other essential aspects needed to provide a secure system in the cloud. I think guidelines can be good if they show what one should look for when evaluating cloud business intelligence. **[Participant 9]**

These extracts indicated that decision-makers were able to use guidelines and checklists in completing some evaluations and were prepared to use these tools to evaluate Cloud BI and other IT solutions.

*vi. Examining the level of knowledge needed to use Cloud BI*

The level of knowledge and skills needed to operate or use the Cloud BI was a major concern among decision-makers, and they suggested this should be another strategy to assess Cloud BI before adopting it. Attestations from two participants reveal that the applications that required a lot of knowledge and skills to operate, posed a security problem when used by non-IT specialists.

Besides checking the security controls in an app, I also want to see how difficult the system is if one wanted to learn to use it. I will avoid any IT solutions with complications regarding installations, subscriptions, and use. I do not want to spend a lot of time learning new technology. Rather, new technologies should be very easy to understand and use to avoid making costly mistakes. **[Participant 4]**

When I get new software, I normally try to understand how it works, its benefits and its setbacks before I adopt it. I start by looking at what I know then explore the app by trying it with my data. Where I find problems, I consult tutorials. If it is difficult to understand and use, I leave it and try another one. **[Participant 9]**

These findings confirm that decision-makers considered the level of knowledge and skills required to use the application as important areas to evaluate. Decision-makers were more likely to avoid adopting Cloud BI, which needed a lot of effort and time to learn to operate or use. The decision-makers were afraid of making mistakes that would risk their chances of making profits. This obliged decision-makers to think of assessing how difficult it was to learn and use Cloud BI. Decision-makers thought that easy-to-learn and use Cloud BI could reduce security breaches by non-IT specialist users compared to one that is difficult to learn.

*vii. Assessing physical security of data centres provided by Cloud service providers*

Some participants were determined to evaluate the security of physical infrastructure, particularly the data centres where the cloud infrastructure would be hosted. Participants were of the view that decision-makers preferred to find out how physically secure were CSPs' data centres against

various natural disasters, and unauthorised access such as burglary. These excerpts indicate the position of participants:

For me, I find the physical security of the cloud very difficult when deciding to move to the cloud because I am not able to access data centres and verify how secure they are. This depends on how much trust an enterprise can have in the provider is. I am eager to have access to the place where my data will be stored to see how secure it is and who has access to data. **[Participant 1]**

**Participant 4** expressed eagerness to, “examine the physical security of computers where the data would be stored while in the cloud to make sure that the computers would be safe from theft where possible”. This assertion indicated that decision-makers were aware that CSPs were located in different countries, and this was to make a physical inspection of data centres difficult. **Participant 10** expresses the same notion,

I am sure that providers take advantage of the fact that we are not able to access them physically. I wish I knew their physical location, particularly those in our cities so that I can check what happens there to be sure of the methods they use to secure data.

**Participant 12** said,

I can say that I have not confidence in cloud technology; I do not like taking chances without assessing the security of the place of storing the data. It is a which for everyone to check if the service provider is capable of proving good protection to computers supposed to store data. I find it strange to imagine that I just upload business information to the web, then go on to use the service without caring exactly where it will be kept.

From QUAL findings, fourteen security evaluation activities were identified and used in the QUAN phase to determine the knowledge about security evaluation in Cloud BI on a 5-point Likert scale rating (Strongly agree = 5, agree =4, not sure = 3, disagree = 2 and strongly disagree = 1). The results for ratings, present in *Table AP4.3 in Appendix J*, were summarised into five categories. The findings show activities that respondents regarded as crucial when evaluating Cloud BI and CSPs. The mean score rating of 4 and above showed that the activity was important in the evaluation process and decision-makers should perform it.

*i. Evaluating data security-related issues in the cloud*

A mean score of 4.0 to 4.4 showed that respondents agreed or strongly agreed that the activity should be used by decision-makers when evaluating Cloud BI. Seven activities were suggested for evaluating data security by decision-makers: 1) checking information asset accessibility publicly by unauthorised cloud users (91.2% respondents, mean score 4.4); 2) verifying if CSP’s employees can access and manipulate enterprise data without permission (84.2%, mean score 4.2); 3) verifying whether the enterprise could migrate its data to another CSP easily, (82.4% respondents, mean score 4.2); 4) identifying and understanding exposure to risk and capability of managing it

(82.5%, mean score 4.1); 5) checking whether processes or function on clouds can be manipulated by outsiders, (82.4% mean score 4.1). Checking the reports of the duration of the unavailability of the cloud to the users was regarded as important by 80.7% (mean score 4.0) of the respondents. Finally, checking reported cases of whether unexpected changes to data/information in a cloud once it occurred was rated as important by 73.7% (mean score 3.8) of the respondents.

*ii. Evaluating security controls and functionality in application Cloud BI interfaces*

Close to 87.7% of the respondents (mean score 4.2) regarded security evaluation as a process in which they were supposed to check whether expected security controls were functioning properly, as claimed by CSPs. The features alluded to were access control, backup, and recovery facilities which are documented in industry security standards and frameworks. The best practice in security evaluation was important among SMEs.

*iii. Evaluating CSP related issues*

Decision-makers perceived security evaluation as a process that required scrutinising CSPs because they played an important role in the adoption and use of Cloud BI. The results show that 91.2% of the decision-makers (mean score 4.3) perceived security evaluation as using security reliability information from various security organisations or publications about the CSPs and Cloud BI. Besides, 81% of the respondents understood security evaluation to mean checking the level of data control an enterprise would have in the cloud (mean score 4.0).

*iv. Evaluating contracts and Service lease agreements*

Participants viewed security evaluation in terms of contracts and SLAs between CSPs and clients. Most of the respondents, 91.2% (mean score 4.2) perceived security evaluation as assessing possibilities of being tricked into signing contracts with poor performing CSPs which will be difficult to correct afterwards. Furthermore, 80.6% of the respondents (mean score 4.0) understood security evaluation as enabling clients to find any conceivable causes of conflict with the CSP in both quality of service and SLAs.

v. *Evaluating financial risk*

The results show that some of the respondents perceived security evaluation as assessing the financial risks that an enterprise may incur by adopting the technology. Close to 76% of the respondents regarded security evaluation as being able to assess financial risks emanating from hidden subscription costs. Security evaluation was seen by 76.2% of the respondents as the ability to check whether financial risks could result from a lawsuit by customers after exposure of data. The mean score of 4.0 for each item confirmed the assertions by participants. Overall, the results show that respondents understood the implementation of security evaluation as simple activities they were able to conduct in their enterprises. These results showed a pragmatic approach to evaluation which required decision-makers to be actively involved, using as much of their limited knowledge as possible to evaluate the technologies they intend to adopt and use. The results show that the scope of security evaluation among decision-makers was very wide.

**Sub-theme 3.2. Description of tools used in evaluating Cloud business intelligence**

Narratives by some participants showed that decision-makers had the basic knowledge of tools and methodologies that could be used for the basic evaluation of IT applications although they did not systematically utilise them. Some participants described how they would benefit from guidelines and checklist when evaluating Cloud BI:

I am familiar with checklists and guidelines but not with models and frameworks, these are a bit advanced and I need more effort to understand and use them...I think a comprehensive and simple checklist can assist me in evaluating cloud services. **[Participant 1]**

I know checklists, particularly for system specifications and requirements which are easy to follow, but besides that, nothing, I am not sure about models and frameworks, some of these things I read about them. **[Participant 2]**

I would suggest that appropriate checklists be developed for this purpose.... I do not like a lot of unnecessary difficult tools I might fail to use **[Participant 9]**

**Participant 6** seemed to be familiar with certain IT models and frameworks though not related to Cloud BI and was quick to point out that they were complicated as they imposed additional demands on users.

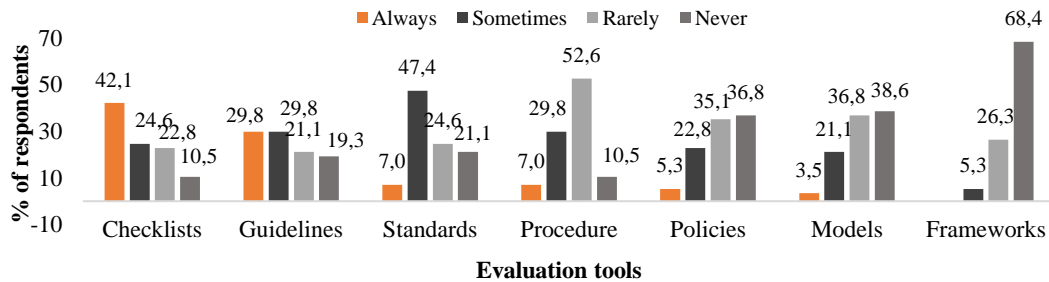
I have tried to research these models and frameworks after I was advised by my friend, an IT specialist with a successful enterprise, but I always found myself overwhelmed with these tools. I do not understand how relevant they are to my situation. You know, I want something simple and straightforward. I do not want to waste time on things I will not be able to use or want me to be reading all the time.

**Participant 4** indicated that the tools were only for large organisations as they could be used by IT specialists, however, appreciated knowing malware scanners and guidelines.

I am not aware of any cloud evaluation tools or models for small businesses because there is no one to use them, maybe for large businesses with lots of computers. I am very good with antivirus, anti-spyware, or guidelines. Guidelines are easy to use in checking what is there, what works and not. Framework... eh, ...I think it is difficult to use because they demand more IT skills which I may not have.

The participants purported to be ignorant of security evaluation tools but elaborated on some of the tools that could be used for scanning malware and assessing applications. The participants expressed the common stereotypical belief that other tools are not suitable for SMEs but LBEs, without understanding how they worked. The attestations by participants revealed that most of the decision-makers had little knowledge about models and frameworks but knew about guidelines and checklists that might be used to achieve similar purposes.

Results from the QUAN phase on the knowledge of methodologies, models, and frameworks used in the evaluation of Cloud BI or any other IT systems are shown in Figure 4.5. Decision-makers were asked to indicate the frequency of use of selected tools and methodologies when evaluating any IT solutions including cloud services they intended to adopt.



**Figure 4.5: Ratings on the frequency of use of selected tools in evaluating IT solutions**

Figure 4.5. shows that the most frequently used evaluation tools were checklists, 24 (42.1%) and guidelines, 17 (29.8%) respondents, respectively. The least frequently used tools were models, 2 (3.5%) and frameworks, 3 (5.3%).

### **Sub-theme 3.3. The importance of understanding security evaluation decision-makers**

Participants indicated three major areas they thought justified the need for decision-makers to understand security evaluation when they decided to adopt and use Cloud BI: 1) decision-makers were accountable and responsible for security issues in the enterprise; 2) the importance of decision making based on evidence and experience, and 3) knowledge and skills in software evaluation to improve security assessment and selection of the most appropriate solutions for supporting business objectives in SMEs.

#### *i. Decision-makers are accountable and responsible for security issues in the enterprise*

SME decision-makers were responsible and accountable for all business operations in their enterprises, and before decisions were made about the technology to be adopted and how it would be used were crucial. Participants 1, 3, 4, 5 and 7's narratives provided reasons for decision-makers to understand the security evaluation of Cloud BI and other emerging technologies. Although participants appreciated the role played by IT experts, they believed that decision-makers were responsible and accountable for all decisions made. Participants highlighted the responsibilities and level of accountability that decision-makers should have in the adoption and use of ITs in an enterprise.

After all, there are those things that you can say I can do and those that need to be referred to experts. While an expert opinion remains good, my judgement is important at the end of the day, so it is important to understand how to assess business intelligence in the cloud as well as other applications found in the cloud.

**[Participant 1]**

I will try to understand all the important aspects of an app that will serve and make the enterprise prosper. I do not think that I need to be an expert in IT for me to be able to select the right cloud app ... but I need to be patient and understand a bit about each app by asking for advice from those who use or understand it better. As a manager, I have the final say on whether to go ahead with the adoption of an app or not. ... I cannot leave this to subordinates. I should be able to tell which app is safe for use by the enterprise, otherwise, we could end up using whatever app is available putting the enterprise at risk. In my opinion, it should be my responsibility to evaluate any IT product before it is used instead of seeking explanations from subordinates after things have gone bad. **[Participant 3]**

Participants believed that decision-makers who understood the evaluation of cloud applications would view security in IT systems in a different dimension and make them more accountable. Although participants appreciated the technical assistance offered by IT specialists, they strongly felt that decision-makers should take a leading role in the evaluation of cloud applications to enable them to justify the selection of certain apps. The following excerpt supports this notion:

I think now is the time we do things differently with little assistance from IT specialists if we are to be successful in business. I am not comfortable with the idea that someone from outside brings software and start testing it with us and probably leave within a day or so when we still do not understand what's going on. I think it is a good practice for me to have some understanding of evaluating an application I want to use so that I start from an informed position. This will allow me to find the application that closely matches the enterprise's business needs. I think giving small businesses a chance to evaluate different IT products, is the right thing to empower them to make their own decisions. **[Participant 4]**

Participants thought that it could be easy for decision-makers who knew security evaluation to understand the selection process better.

Even if one were to consult an IT specialist, it will be from an informed position, unlike the current situation where we work on suppositions and speculations. Leaving our technological needs in the hands of consultancy is always wrong as some may have malicious intentions that may put business operations and reputation at risk. **[Participant 5]**

*ii. Promoting evidence and experience-based decision making*

The findings showed that knowledge and skill in security evaluation were generally important for SME decision-makers to make decisions about security in Cloud BI based on existing evidence and personal experiences. Participants expressed that decision-makers should have clear insights into the benefits and vulnerabilities of Cloud BI to justify the selection of cloud services. The extracts by Participants 1 and 2 confirm how important practical knowledge and experience of security evaluation were in decision making.

I need to know and understand beforehand how safe the cloud technology I am intending to use is. When one understands or knows how to perform a simple evaluation of IT, apps, particularly in cloud technologies, then will have an upper hand over service providers. You can always compare what they are offering against the risks that you already know and can even make quick research on threats to the technology you want to adopt. **[Participant 1]**

Relying on IT salespersons may not be good enough to provide the information needed for making key decisions on the safety of the system being evaluated. Some specialists give information that is biased toward products or solutions of their choice, or they are promoting. At times, it is important to be independent in decision making concerning some IT products. I think a businessperson should learn to look for relevant information about any product, then use that information to decide whether the product is suitable for the business **[Participant 2]**.

These attestations show how important it is for decision-makers to have experience in Cloud BI evaluation instead of accepting solutions at face value, without evidence on the safety of the enterprise information systems' assets. Some participants expressed that decision-makers actively involved in the evaluation process could make informed decisions based on their knowledge about different types of security features and implementation in the Cloud BI. Therefore, the knowledge and experience of security evaluation acquired by decision-makers are important in supplementing

expert knowledge and advice which is difficult to come by. This extract further supports this line of argument:

Although I get advice from those who are familiar with the technology, I still need to assess the system to make an informed decision on whether to adopt it or not. Yes, I think that all prospective users of new IT solutions should be able to evaluate the solutions they want to use one way or the other. **[Participant 4]**

Participants believed that self-reliance among SME decision-makers in evaluating Cloud BI was essential in the escalation of the adoption of Cloud BI. Some expressions by participants prove that decision-makers who have experience and knowledge in security evaluation stand a better chance of adopting and using the technology.

I need to understand the evaluation to reduce the costs of hiring other people to do that for the enterprise. I think that managers should be self-reliant when it comes to decision making concerning the selection and use of new IT systems. Waiting for advice from experts will always cause the manager to have other thoughts leading to the hesitation to uptake the technology. **[Participant 9]**

Currently, most of the new applications are acquired from the web and this requires decision-makers to evaluate the Cloud BI and other cloud services to get these from safe sources. **Participant 3** thought that changes brought by cloud computing on how services were obtained required managers to be familiar with security issues in the cloud if they were to adopt secure Cloud BI.

The tradition has been that when an enterprise wanted to adopt IT products, it would contact a salesperson/vendor and get the product as well as the relevant training. Things have changed now and require business people to be actively involved in the process of IT product selection and learn by themselves. **[Participant 3]**

This narrative suggests that decision-makers should have first-hand experience and evidence of the safety of the technology to make an informed decision regardless of having advice from IT specialists. They need to supplement expert knowledge with their own experience of security evaluation.

*iii. Good knowledge and skills in application evaluation improve security assessment in small and medium enterprises*

Participants' attestations indicate that a better understanding of Cloud BI evaluation by decision-makers was important in improving their knowledge and skills in security assessment, which could subsequently lead to the selection of secure applications that meet enterprise business needs. The excerpt supports the above notion:

I need to be informed about security issues and how to deal with them. I try to go around simple problems in securing my data without involving other people whom I do not trust. It is wise for me to have baseline



knowledge and skills in evaluating software so that the right decisions are taken before one adopts the wrong product. Even if a salesperson was to visit me, I must have my way of judging the suitability of the application being offered, otherwise, one can get committed to the wrong one and risk a lot of investment. **[Participant 1]**

The sense of being independent of salespersons and software vendors is an encouragement for decision-makers to seek means to acquire basic knowledge and skills in security evaluation so that enterprises benefit from new technologies. Some participants were convinced that SME decision-makers who appreciated security evaluation were more likely to personally check and verify the suitability of Cloud BI against their security expectations. The following two excerpts convey the notion above.

Security is essential in IT and every businessperson who uses IT should at least have some understanding of how to check for basic security functionalities. When it comes to the adoption of cloud technologies where assistance is scarce, there is a need for one to understand how security is evaluated, especially where it concerns users. Businesspersons are anxious about how to recover lost data, system crashes, disruptions of service and theft or corruption of data. **[Participant 6]**

My view is that no matter how secure a system could be if the user does not understand its security features in it, the system could easily be compromised. I believe decision-makers should understand how to conduct basic security checks or assessments for IT solutions beforehand to prevent unnecessary problems in the future. Once one understands how to evaluate security, I think one will be able to assess the financial risks associated with an IT solution. **[Participant 10]**

The assertion by **Participant 9** reveals how concerned decision-makers were about improving their knowledge in security evaluation so that they assess basic security features in the system:

I am convinced that one who can evaluate security in IT applications will not be greatly influenced by service providers. I will take them on the task to explain several things crucial to the functionality and safety of the software ... it is good that before one adopts and uses new technology, one should understand how it works as well. It is wise for a person in my position to be able to assist in the selection of appropriate cloud services for the organisation as this will assist the organisation in safeguarding against many risks. It is my responsibility to make the right decisions on which technology to use and to see to it that it is safe.

The knowledge of security evaluation empowers decision-makers to make their assessments, compare their findings with those of experts and then make an informed decision based on many perspectives rather than on biased ones. In this study, participants acknowledge the importance of expert opinions but think the decision-makers were supposed to be actively involved to improve the assessment of Cloud BI.

### **Sub-theme 3.4: Effects of limited understanding of the evaluation process on the adoption of Cloud BI**

Besides the positive aspects of understanding security evaluation, participants' attestations revealed the negative effects of limited understanding of security evaluation on the adoption and

use of Cloud BI. The effects of limited understanding of security evaluation were found to lead to the selection of inappropriate IT solutions and reluctance in the adoption and use of Cloud BI by SMEs in general.

*i. Leads to the selection of inappropriate technology solutions*

Participants attested that limited knowledge and skills in the evaluation of Cloud BI by decision-makers increased the possibilities of selecting inappropriate IT products, solutions and wrong CSPs.

It is difficult to select the right applications in terms of business needs and security requirements because we always think that everything, we need to use should be recommended to us by IT specialists, now service from IT specialists is found online, making it difficult to tell which one tells the truth or not. **[Participant 2]**

This is common sense... with little knowledge, impulsive decisions lead to the selection of application of poor quality applications. **[Participant 3]**

.. we are not able to do our evaluation and end up asking many people who do not understand the security of cloud applications... the result is following the dominating idea which may lead to the selection of an inappropriate application, which would gather dust because it cannot be used at all. **[Participant 11]**

Quantitative results shown in Table 4.8 further confirm the findings from the QUAL strand.

*ii. Reluctance in the adoption and use of Cloud BI by SMEs*

Some of the participants were of the view that poor understanding of security evaluation among decision-makers led to a reluctance to adopt and use technology in SMEs. Narrations from some participants suggest that being ignorant or uninformed about technology prejudices SMEs in many ways, as wrong decisions to not adopt the services are made.

A well-informed person will make better decisions quickly on whether to adopt cloud services. I am saying that, if I had a better understanding of security evaluation in cloud business intelligence, I would have made better decisions towards the adoption of the technology long back. **[Participant 3]**

When there is a new technology which you have no idea of how it works and its pitfalls, then you have many problems in deciding whether to use it or not. This is made worse by having contradicting views from different sources of information around you. I think it is safe to wait and see how friends use the technology before using it. **[Participant 8]**

If I am in doubt about the safety of the technology, I will not recommend its use. I am sure that my inability to decide on which application is suitable is influenced by my poor knowledge of assessing security in cloud applications. I am afraid of choosing the wrong applications which can affect the operations of the enterprise negatively. Without adequate knowledge about the security of online IT services, it becomes difficult for the organisation to commit itself. **[Participant 9]**

Results from a QUAN phase depicted in Table 4.8 show the ratings on the importance of understanding security evaluation among decision-makers in SMEs. The ratings were based on a

5-point Likert scale (strongly agree = 5, agree =4, not sure = 3, disagree = 2, and strongly disagree = 1).

**Table 4.8: The importance of decision-makers’ knowledge and skills in security evaluation**

| Item  | Rating (n = 57)      |             |                |                |                         | Mean | Std. Dev |
|---|----------------------|-------------|----------------|----------------|-------------------------|------|----------|
|   | Strongly Agree f (%) | Agree f (%) | Not Sure f (%) | Disagree f (%) | Strongly disagree f (%) |      |          |
| A good understanding of security evaluation makes decision-makers accountable and responsible for security issues in the enterprise | 24 (42.1)            | 27 (47.4)   | 5 (8.8)        | 1 (1.8)        | 0 (0)                   | 4.3  | 0.7      |
| Poor understanding of the security evaluation of Cloud BI leads to the reluctance in the adoption and use of Cloud BI by SME        | 32 (56.1)            | 17 (29.8)   | 5 (8.8)        | 1 (1.8)        | 2 (3.5)                 | 4.3  | 1.0      |
| A good understanding of security evaluation is important for decision making to be based on evidence and experiences                | 21 (36.8)            | 27 (47.4)   | 7 (12.3)       | 1 (1.8)        | 1 (1.8)                 | 4.2  | 0.8      |
| Good knowledge and skills in software evaluation by decision-makers improves security assessment in SMEs                            | 22 (38.6)            | 26 (45.6)   | 8 (14)         | 1 (1.8)        | 0                       | 4.2  | 0.7      |
| I can only recommend the adoption of Cloud BI when I am well-knowledgeable in security evaluation of the technology                 | 22 (38.6)            | 28 (49.1)   | 0              | 3 (5.3)        | 4 (7)                   | 4.2  | 0.8      |
| Only decision-makers with good knowledge and skills in Cloud BI evaluation can recommend the adoption of technology                 | 25 (43.9)            | 23 (40.4)   | 4 (7)          | 3 (5.3)        | 2 (3.5)                 | 4.2  | 1.0      |
| Poor understanding of the security evaluation of Cloud BI leads to the selection of inappropriate technology solutions              | 24 (42.1)            | 25 (43.9)   | 3 (5.3)        | 4 (7)          | 0 (0)                   | 4.2  | 0.8      |
| Decision-makers in SMEs can be held responsible for a breach of security of the data they store in the cloud                        | 23 (40.4)            | 23 (40.4)   | 7 (12.3)       | 2 (3.5)        | 2 (3.5)                 | 4.1  | 1.0      |
| Only experts in security can evaluate Cloud BI and recommend their adoption   | 24 (42.1)            | 23 (40.4)   | 5 (8.8)        | 4 (7)          | 1 (1.8)                 | 4.1  | 1.0      |
| SMEs are only responsible for data security in a private cloud  | 3 (5.3)              | 12 (21.1)   | 21 (36.8)      | 12 (21.1)      | 9 (15.8)                | 2.7  | 1.2      |

The results in Table 4.8 show how important basic knowledge and skills in evaluating Cloud BI were for decision-makers to select the appropriate and secure applications. A mean score rating of 4 and above indicates that respondents agreed with the aspect being measured. Most of the respondents, 89.5% indicated that a good understanding of security evaluation promoted accountability and responsibility for security among SME decision-makers. This was consistent with 85.9% of the respondents who agreed that the poor uptake of Cloud BI by SMEs was due to

a poor understanding of the evaluation of IT solutions by decision-makers. Close to 83% of the respondents indicated that a good understanding of security evaluation promoted evidence-based decision making. This was supported by about 84.2% of the respondents who indicated that good knowledge and skills among decision-makers were essential in improving security assessments in SMEs. Nearly 88% of the respondents affirmed that good knowledge and skills in security evaluation were needed for decision-makers to recommend Cloud BI to their enterprises.

Furthermore, 86% of the respondents indicated that decision-makers' poor understanding of the security evaluation consistently led to the selection and recommendation of inappropriate IT solutions for their enterprises. This had a negative effect in that decision-makers would be reluctant to recommend the adoption of Cloud BI because they feared being held responsible for making wrong decisions that would lead to data security breaches in the cloud, indicated by 80.8% of the respondents. Due to the fear of making wrong decisions, 82.5% of the respondents would prefer IT specialists, to make recommendations.

The findings indicate that decision-makers understood the importance of knowledge and skills in the evaluation of IT solutions before adoption. The findings emphasise the need for decision-makers to be pragmatic and get involved in application evaluation so that they can complement advice from experts. The overall impression was that decision-makers had positive feelings about the role of decision-makers in security evaluation so that they could make meaningful decisions with regards to the selection of the Cloud BI to adopt.

The above findings were confirmed by Chi-Square test results in Table AP4.5, Appendix J, which show a significant association between the importance of knowledge of security evaluation in Cloud BI and the level of education of the respondents at p-values of less than 0.05.

### **Sub-theme 3.5: Suggestions on security evaluation considerations**

Participants were asked what they would consider important when evaluating cloud applications such as Cloud BI. The responses by participants were analysed and categorised into five areas that decision-makers should consider when evaluating Cloud BI.

**i. Data and application security, portability, and cloud interoperability in the clouds**

Some participants attested that decision-makers must prioritise data and application security, portability, and cloud interoperability. Excerpts from participants 6, 7 and 3 reveal that data and application security in cloud and cloud interoperability were major areas that decision-makers felt should receive much consideration when evaluating Cloud BI.

Before I adopt IT solutions such as cloud business intelligence, I need to ensure it was safe to use and that the enterprise data and information would be safe, especially when it is hosted on the web where the chance of losing information is high even for large organisations. I will be happy if I were to get assistance to go around this problem because the data is essential, and it must be protected by all means. **[Participant 6]**

The thing is that one needs to be careful before adopting online applications, particularly these cloud services where there are chances of exposing data to many cyber threats which may end up making the company lose customers and money. I want to maintain good standing integrity with customers all time. I think I should focus my efforts on finding how secure the cloud is beforehand, I will try to verify with many providers how secure the system is. **[Participant 7]**

These two excerpts indicate that decision-makers were aware of the dangers surrounding data migration and management in the cloud and therefore were precautionous in prioritising the assessment of many forms of data security while evaluating Cloud BI regardless of their limited ability to conduct an evaluation. Data recovery is another important aspect of data security that another participant indicates should be evaluated:

I will be obliged to determine how the CSP provides for the recovery of data in case of system failure together with how they would detect and mitigate attacks that may occur. **[Participant 3]**

The fate of enterprise data and information after leaving the cloud was an essential security consideration as indicated by **Participant 3**.

If I can leave the service provider, the application should delete all data and information from the cloud storage so that no trace of it is left for use by competitors. I should have a way of checking that all my data was removed from the provider whenever I leave. Secondly, I am not sure whether the providers use databases similar to those we use so that data formats do not change when migrating data.

The findings show that participants were worried about the aftermath of a discontinued subscription to a CSP. Decision-makers feared leaving behind copies of their data files that could be used for malicious purposes by unscrupulous CSPs after unsubscribing. This underlines the importance of data as an asset in SMEs regardless of how they used it.

Furthermore, data portability was considered important, and participants felt that decision-makers should focus on this aspect when evaluating security in Cloud BI. Participants raised concerns that

the migration of data might require conversion to another format and could render the data unusable in the future, a scenario that decision-makers were sensitive about and were trying to avoid or prevent.

My first concern will be checking if the cloud application is compatible with the data I want to move to cloud storage. I know data is sometimes easily corrupted when converted to another format. I can also check that the new system can open the data files without compromising their correctness. It is important to check if the data will stay unaffected when uploading to the cloud and for future use. My problem is that I am not sure how to check these because even if I were to ask the provider, I will be assured that the solution can do all those things but only to discover after subscribing that it was not true. **[Participant 3]**

...one should check the data compatibility with application requirements. If we upload files to the cloud, we should be able to get them back in their original form with all data in place. I am not prepared to be caught off-guard during system maintenance and upgrade which usually lead to data unavailability. **[Participant 8]**

These excerpts show that data portability and system compatibility are security risks that must be considered when data is moved from on-premise applications to Cloud BI and back.

Cloud interoperability was recommended for consideration during the Cloud BI evaluation process. The utterances by participants 1 and 9 expressed the idea of cloud interoperability that suggests that decision-makers should consider the possibility and ease with which the enterprise moves data and information from one cloud provider to another with a different infrastructure.

I am always worried about moving data among cloud providers using different technologies and applications. It is bad to discover after signing a contract that data cannot be moved directly from one provider to another. This will mean that one stays with the same provider for a long time... one cannot bear the idea of getting stuck to a poor performing provider. **[Participant 1]**

I am not sure whether the providers use the same cloud technologies across different countries because I have seen that many solutions are not South African. Being the case, I need to look at the possible complications that might arise when I decide to move to a local provider who may use different cloud technologies. You know circumstances do change and you find yourself being stuck to one provider who makes things difficult by using a unique system that restricts the enterprise from retrieving its data or even discontinuing the services due to such complications. **[Participant 9]**

The two extracts show that decision-makers were concerned with the ability of an enterprise to move data and applications between two CSPs who used different cloud technologies, particularly from an international provider to a South African.

## **ii. Operational and security functionalities and ratings of Cloud business intelligence**

Attestations by some participants conveyed the notion that decision-makers expected certain security functionalities to be available in Cloud BI. It was suggested that decision-makers should

consider checking for the necessary operational and security functionalities, their deployment, and utilisation before the adoption.

It is wise to have a closer look at the history of cloud applications on offer in terms of security and privacy. ... importance features used to protect data when moving it, processing and storing it in the cloud.... Each application being used could be evaluated by other users and the information can be found on request or by research on the net. **[Participant 3]**

I can look at the key features including security controls whether they function to meet our business needs. I may want to have hands own trial of the software to check things like the interface whether it is user friendly, safe and allows users to log in and if their use is safe. **[Participant 5]**

Checking for self-service features in the cloud app is also important. I do this to make sure that the functionalities offered are configured so that I can easily use them by myself and without assistance from IT specialists. **[Participant 7]**

Participants thought that the security ratings of the cloud services were very helpful and should be considered in the evaluation process. Participants acknowledged their role as decision-makers by carrying out the evaluation using whatever information and resources which were at their disposal. Although ratings of Cloud BI by security organisations can provide a guide to how secure the system could be, these cannot be the only criterion used for the selection of the technology.

### **iii. Financial benefits and risks of the cloud business intelligence systems**

Enterprises usually make decisions to adopt and use technologies when they expect to get more financial benefits than losses, a notion highlighted by participants in this study. Participants 1 and 4 express financial risks, from security breaches to application vulnerabilities and system unavailability, have an adverse effect on the finances of the enterprise.

It is better to look at the benefits of the apps to our business interests first and then look at the pitfalls. I do not want to be blinded by benefits that may not materialise, then overlook risks that could surface after the enterprise is using the application. **[Participant 1]**

My advice to enterprises is that they must consider possible financial risks caused by these cloud business intelligence apps. If I were to subscribe to a service provider, I will first seek assurance that if there is a disruption, the enterprise must not be affected financially in any way. **[Participant 4]**

**Participant 5** was of the view that decision-makers should consider financial risks associated with additional subscription fees imposed on the enterprise after adopting a free app.

... besides the ease of use of the IT app, I also look at the financial implications of adopting the app, what financial risks are likely to be incurred if a free application prompts for payment when in use and then one cannot run it. I look for free or cheap services without hidden financial implications like additional subscriptions. If the CSP asks for additional payment to enable other functionalities, I leave the application to

protect the enterprise from financial expenses. Who knows, these guys can keep on asking for more money as long as one pays.

Another participant indicated that decision-makers should take account of financial risks if they lost control of sensitive data on CSPs.

I also realised that when I stored data in the cloud, I was likely to lose control of it to the provider and this may have financial implications if the employees of the provider access and leak the data. I heard many stories about data exposure by hackers and employees of providers, particularly with large companies who use the cloud to store information. I think it is good for one to have at least two or three solutions that are close to the needs of the organisation from which to select. **[Participant 6]**

The findings show that SME decision-makers were mindful of probable unscrupulous practices by some CSPs and employees that could result in financial risks, which, SMEs always try to avert. The excerpts reveal that decision-makers were always quick to consider financial risks arising from threats and vulnerabilities in the cloud which were likely to negatively affect their profits. This makes decision-makers constantly suspicious of CSPs and their employees who could access the enterprise data and, as a result, would require assurance from the CSP on the security. The narratives suggest that decision-makers seriously consider the various financial risks of using Cloud BI even if the benefits outweigh the former.

#### **iv. Assessing the level of access to data and control in Cloud BI that the users and CSPs have**

Another consideration for evaluating security in Cloud BI was to assess whether CSPs accessed enterprise data and the level of control the enterprise had. The response by **Participant 2**, “I prefer to find out how much control on data I will have in the cloud application before I adopt it,” shows that the participant thought it was important to ascertain the level of control that the CSP would have over data.

According to **Participant 7**, decision-makers need to ascertain the extent to which the CSP employees will have access to enterprise data and the types of operations they can perform without compromising the data.

I know that it can be very difficult for me to stop the providers from accessing our data, but at least they need to tell the clients the extent they will access the data and the types of operations they will allow their employees to have on our data.



Attestation by **Participant 9** suggests assessing control of system updates or upgrades, processes that affect system availability and data integrity, particularly during peak times of business operations.

I am very particular with the control I will have on the data, software upgrades and updates of the system. I want to know how much control I will have on system updates and maintenance so that I can schedule these during an off-peak time, otherwise, the enterprise could be in the mess of the vendor who can run updates any time and disrupt business operations.

The attestations show that decision-makers should evaluate Cloud BI before adoption.

#### **v. The environment where the Cloud BI will be used**

The environment in which the BI applications were to be used was highlighted as another important area for consideration during the evaluation process. The environment includes the cloud deployment model, other cloud tenants, the SMEs and CSP employees, as well as the cloud environment, namely, the web, by which the app will be accessed.

One will have to consider the environment in which the system will be used and those who will use it whether they need much training, but I normally do all data management. It is also important to make sure that no one from outside will have access to the data, by checking whether the cloud business intelligence is secure. I look at the sensitivity of the data and decide which one to put on the cloud. **[Participant 7]**

At times it is important to consider where the application is to be used and by whom. I think the web is ideal for easier access but unsafe for the data as it can be exposed to many threats of which the enterprise may not be aware. By the time one comes to know about the threats, it will be too late to protect the system. **[Participant 8]**

The cloud is a complicated space for some novices in IT usage. It is a big issue to consider whenever you face challenges brought about by these new changes. I do not think small businesses will be able to cope with these changes which happen overnight. A few years back it was easy to manage your data on a PC but now things keep changing as increasingly new technology comes and go. It has become so competitive that we need to compromise and use the technology in this confusion but take care of not exposing sensitive data to cyber threats. **[Participant 12]**

The findings from the QUAL phase were further investigated in the QUAN phase in which respondents were asked to rate the importance of each consideration to the evaluation of Cloud BI. *Table AP4.4 in Appendix J* displays the ratings of each security consideration aspect based on a 4-point Likert scale (very important = 4, important = 3, less important = 2 and not important = 1), alongside the mean score for each. The results show that data and application security and portability and cloud interoperability were regarded as essential consideration aspects of the security evaluation process, as indicated by high mean scores of 3.5 to 3.7 and ratings by at least 91% of the respondents. This implies that decision-makers should assess these aspects of cloud services during the evaluation process. Between 74% and 89% of the respondents indicated security considerations such as data

backup and recovery of the application, firewall configurations, password protection, legal and administrative issues, human resources security, vendor or provider reliability, security features of application interfaces, compliance with national and/or international legislation and the availability of security guideline from CSPs as being important. Considerations believed to be least important by 63% to 73% of respondents were responsibilities and liabilities of the enterprise, organisational security and risk management, and physical security of providers.

#### **4.1.5. SRQ3: What challenges do decision-makers face when evaluating Cloud BI?**

Theme 4 and three sub-themes are presented in this subsection supported by results from the quantitative analysis.

##### **4.1.5.1. Theme 4: Challenges faced when evaluating cloud business applications**

Participants expressed various views on the challenges faced by SME decision-makers when evaluating Cloud BI or any other cloud major service. The three challenges which emanated from the attestations of the participants were discussed under respective sub-themes

##### **Sub-Theme 4.1. Limited knowledge and skills to evaluate Cloud business intelligence among decision-makers**

Findings from the interviews indicated that decision-makers had limited knowledge and skills in assessing Cloud BI and this stifled the effort to evaluate cloud technologies. Knowing cybersecurity threats was not enough for decision-makers to evaluate cloud applications. Decision-makers lacked technical know-how in assessing the key areas they could have wished to, and this was made even more difficult by many similar Cloud BI available. A few excerpts support this finding:

For a person like me, with limited know-how about cloud technologies, makes it difficult for us to decide which cloud business intelligence is safe and easy to use. My IT skills are limited to valuate IT solutions. I am afraid of making mistakes by choosing something which appears appealing but hiding threats. With such many similar cloud services, I find it difficult to choose ....and I have very little information about each product.

**[Participant 4]**

Concerning cloud business intelligence, there is a lot of stuff out there that I can hardly know whether it is secure or not. It is difficult to distinguish between genuine solutions from imitations. The bottom line is that I am not able to determine which service provider is suitable for us, and how secure the service is.

**[Participant 6]**

Business intelligence on its own might be difficult to use depending on a person's capabilities, what more if now in the cloud, I face many security challenges to deal with. I feel that enterprises can face several security problems because of malware on the web. It is difficult to tell the extent to which data and information in the cloud would get enough security **[Participant 7]**

Limited knowledge and skills to evaluate Cloud BI led to time-wasting in assessing a single solution or CSP, thereby delaying the decision-making on the adoption of the technology.

I take a long time to assess because I consult a lot to make sure that I adopt the appropriate technology. If I have not fully understood the IT application, I delay the adoption of the technology. I try to make it a point that the right solution is selected although it may take a long time. **[Participant 9]**

Participants went on to express that due to limited knowledge, coupled with rapid changes in IT applications, decision-makers were unable to determine which applications were safe and uncompromised without relying on IT experts, who are difficult to find, particularly in remote towns. These excerpts attest to this:

I cannot tell which online applications were once compromised...or hacked ...to know the vulnerabilities in the cloud, they are to be deployed. There is nothing much I know about evaluation that can assist in selecting the most appropriate cloud business intelligence. It is difficult to find suitable and reliable IT specialists around this place who can assist just like that. Cloud services are difficult to evaluate without enough tools and information on what to look for. **[Participant 8]**

Cloud computing technologies change rapidly, giving potential adopters limited opportunities to learn and adapt to the technology. These challenges negatively affected the efforts of decision-makers to assess and select suitable solutions that meet the business goals. This assertion illustrates such sentiments:

... we face selection challenges related to the changing nature of cloud technologies. I think there are high risks in adopting cloud business intelligence as it is still new and to be understood by small business enterprises. I do not think that it is possible to assess all of them to identify the most appropriate one. We need some assistance on how to select cloud applications since we are not able to discuss in person with vendors as is the case with traditional software. **[Participant 13]**

#### **Sub-Theme 4.2. Ignorance or lack of suitable tools for use by small and medium enterprises in evaluating cloud applications**

Some participants expressed their ignorance of suitable tools to use for evaluating cloud services. Excerpts from participants 1, 2 and 5 confirm that due to the ignorance of the existence of security evaluation tools, decision-makers faced challenges. The lack of suitable tools to explore and assess Cloud BI for adoption by SMEs also compounded the problem. According to the participants, it was difficult for SMEs to do a proper assessment.

I am not sure if there are suitable tools and procedures to guide small enterprises in selecting cloud services. I think small businesses are placed in the same category as large businesses regarding IT applications. It is difficult to assess cloud business intelligence because the existing tools are advanced for small businesses who are struggling in many areas with emerging technologies due to the lack of specialists. **[Participant 1]**

There is a lot of new technology for all types of businesses, but it is difficult to decide which one to use because we cannot use what large organisations are using. We lack technical knowledge in using the tools they use... Everything seems to be assumed and prescribed to us. I am not sure if there are tools for small businesses for evaluating the cloud instead of being told by the word of mouth that it is safe and good for us to use. **[Participant 2]**

It is difficult for small businesses to select cloud services because we are not able to evaluate them properly... I have noticed that available tools meant for cybersecurity evaluation are difficult for us to use. We do not have enough skills to use the tools unlike in big organisations that have IT people and very good IT equipment. Regarding us small organisations, everyone thinks that it is easy to follow large businesses even if there are big differences in IT resources and business needs. **[Participant 5]**

### **Sub-Theme 4.3. Challenges of getting relevant Cloud BI information from CSPs and vendors**

Participants expressed the difficulties faced by SME decision-makers in getting relevant and useful information from respective CSPs and vendors that they would use for evaluating cloud solutions. The attestations by participants 4, 10 and 11 indicate that participants were sceptical of getting the information needed and whether they would be able to use it effectively for evaluation purposes. Participants indicated that CSPs either misled clients by giving them outdated information or were not forthcoming with information:

In some cases, when you request information from service providers, they always try to cover up for their weak side and tell you what they think will make you happy and sign up for their services. You can only realise after being committed to the service that you have made a costly mistake that you will not be able to correct. **[Participant 4]**

Getting appropriate information about these applications over the net proves to be difficult with so many providers making similar offers but providing little information about the applications. I have seen that some providers attract potential clients with fancy marketing language but offer services with deplorable results. I am not saying that all service providers on the net are like that. I am just saying that one should exercise a lot of caution before losing money to cybercriminals like scammers who are always very good at taking advantage of ignorant users. **[Participant 10]**

**Participant 11** observed that some CSP websites were rarely updated, making it difficult to determine whether the information they contain was still relevant or not.

In many cases, some providers' sites are never updated for a while. I am not sure whether the solutions and services they offer still exist or have become useless. ... one is tempted to shun such providers, but the trend is noticeable in many situations where the offers are too exaggerated making it difficult to tell from the little information available how appropriate is the service.

The three citations indicate how deeply the issue of lack of information about Cloud BI affects the efforts by decision-makers to evaluate existing cloud solutions and services. Lack of current

information about applications may cause decision-makers to delay the evaluation process, which subsequently affects the adoption of the technology.

The three categories of findings in this sub-theme on challenges in the evaluation of cloud applications were investigated in the QUAN phase by asking the respondents to indicate how serious they perceived each challenge. The rating was based on a 4-point Likert scale rating. The results of the perceived seriousness of each set of challenges are presented in *Table AP4.6 in Appendix J*. The results reveal that factors related to lack of knowledge and skills in conducting an evaluation were perceived as the main challenges by most of the respondents, 70% to 96%. An average mean score of 3.3 showed that limited knowledge and skills needed to evaluate Cloud BI applications was a serious challenge that decision-makers had to contend with for successful adoption and use of the technology. The results showed that at least 70% of the respondents indicated that decision-makers required knowledge and skills to assess physical infrastructure, identify vulnerabilities in the cloud environment and flaws in Cloud BI applications, use existing tools to assess financial risks associated with a cloud, and interpreting SLAs and legal issues involved. The results also show that being ignorant or a lack of tools and methodologies suitable for evaluating cloud applications was perceived as a serious challenge as well, as indicated by 67% of the respondents with a mean score of 3.1. The findings indicated that decision-makers were not sure about existing tools they could use to evaluate cloud services. Because of these, decision-makers faced challenges in evaluating key issues, such as survival of CSPs, the meeting of contractual obligations, reliability of Cloud BI applications, testing security controls in Cloud BI applications, and assessing how data from different clients were managed in the same cloud space. Lack of relevant information on how to evaluate Cloud BI applications was another area perceived as a serious challenge in the adoption of the technology by between 61% to 86% of the respondents, with a mean rating of 3.0. The finding indicates the importance of historical and current information about Cloud BI applications and CSPs in the evaluation process. This implies that decision-makers were finding it difficult to get the information they could use to evaluate the cloud within their level of understanding. Such information included security breaches in a cloud, a full history of CSPs, their physical location, and how they managed risks in previous breaches. This implies that when this information is made available to potential clients, they could use it for evaluation purposes.

#### **4.1.6. SRQ4: What do decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises?**

The findings for this SRQ are presented as Theme 5 and its four sub-themes and were substantiated by interview experts and results from the QUAN phase.

##### **4.1.6.1. Theme 5: Knowledge of tools used to evaluate security in cloud business intelligence**

The knowledge about the tools and methodologies used in evaluating IT solutions among decision-makers were vital in the formulation of the framework. Participants were asked to elaborate on any models or frameworks used for evaluating or selecting Cloud BI and any cloud services they were aware of. The findings were organised into three sub-themes.

##### **Sub-theme 5.1. Description of components of the security framework for evaluating Cloud BI by SMEs**

A few participants indicated that an appropriate framework should be composed of rules, checklists, policies, instructions, and functionalities. Other participants tended to repeat answers to previous questions or simply indicated that they did not have any idea.

##### **i. Basic components of a framework that meet the business needs of small business enterprises**

Participants indicated the components of a security framework for evaluating cloud services as simple guidelines, checklists, policies, and instructions. This is revealed by extracts:

I am not sure about the framework, but I am certain that we need something to use to check if the application we want to adopt is safe and ... also it does what we expect. I would suggest something simpler for us who are not using IT so that even if it is used by IT specialists, we can understand what they are doing and the results they get ... I should have clear ideas of what I should look for security controls in a cloud application. ... some guidelines and checklists of general things to expect can be a starting point. I will have to decide the criteria on which to base the evaluation and which can be used with other cloud services. **[Participant 1]**

I think we should have basic guidance on how to identify good cloud applications. It should tell us what to look out for in terms of security in a simpler way. I think we need to know where to start and what to look for in each solution. It should also guide us on identifying which providers are more likely to be secure and how to deal with problems if we are in a fix. **[Participant 2]**

Another participant optimistically suggested that a security evaluation framework should provide certain measures on which decision-makers should evaluate the cloud applications:

Because an evaluation is essential, I think the framework should have a list of items used as some criteria for what we should look for from a product, how the product works and how to use it. It should also guide the user on how to solve problems related to the app if it stops functioning properly. **[Participant 3]**

The main important component should concern guidelines and checklists on what the users should check for on the solutions, it should focus on security features in the app and threats likely to be found in the cloud. **[Participant 6]**

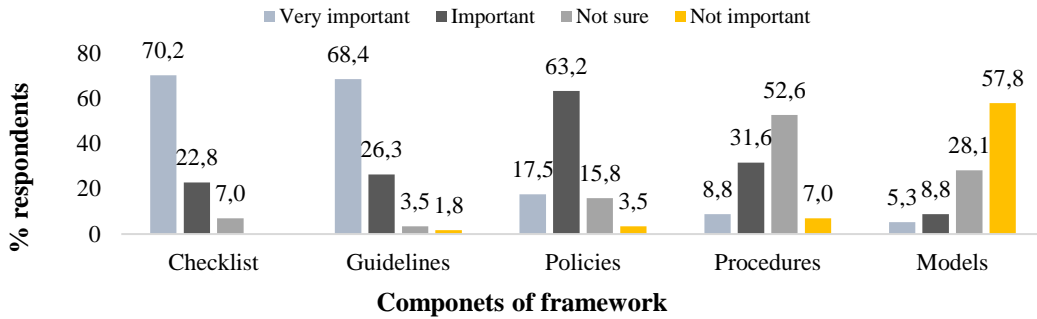
The extracts reveal that decision-makers perceived the components of the security framework as user-friendly guidelines, checklists, or policies with simple instructions to be followed by less or non-technical persons. The extracts further reveal that decision-makers dislike reading long documents and using complicated tools, models, or frameworks. There were high expectations by the participants on what the security framework should do for them.

The expressions by two participants reveal that a security framework should enable the decision-makers to check for a variety of functionalities in the Cloud BI. For example, participants 2 and 3 believed that a security framework should have basic features for easy assessment of Cloud BI to enable decision-makers to select the most appropriate application.

I should have standard guidelines or policies to guide the user in identifying which app is suitable and which basic security features to look for in the cloud business intelligence. **[Participant 2]**

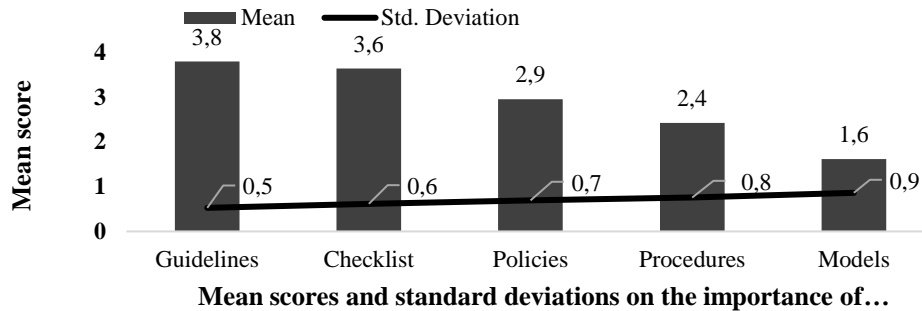
The framework should provide me with the steps to perform when evaluating a cloud product, what I should focus on, and how I should do it in simple terms. There are those things that are similar in all solutions and others which are specific to certain solutions. I will be happy if the tool can show me how to distinguish between fake and real solutions before selecting one. Service providers are fond of promoting products and exaggerate some capabilities. **[Participant 3]**

The respondents indicated their opinions on the importance of guidelines, checklists, policies, procedures, and models as components of a security framework for evaluating Cloud BI by SMEs. A 4-point Likert scale (very important =4, important = 3, not sure = 2, and not important = 1) was used. The results are shown in Figure 4.6 as frequency graphs.



**Figure 4.6: Perceived important components of a security framework**

The results show that the checklist and guidelines are perceived as essential components of the security framework by at least 68% of the respondents, while the lowest number of respondents, 5.3%, viewed the models as very important. Most of the respondents understood a security framework as having more checklists than models. Results in Figure 4.6 are supported by the mean scores and standard deviations in Figure 4.7.



**Figure 4.7: Mean scores on perceived components of a security framework**

The mean score results show that guidelines (3.8) and checklists (3.6) were rated as important components of security frameworks with models (1.6) being the least important components. The results confirm that respondents believed that SME owners were more familiar with guidelines, checklists, and policies compared to procedures and models, although their usage was limited.

**Sub-theme 5.2. Opinions and views on the uses of the security framework**

Opinions and views from participants reveal that decision-makers perceived the use of a security framework as being for: 1) checking data security, functionalities, hidden threats, and vulnerability



in the Cloud BI; 2) making the selection easy and giving directions for the safe use of Cloud BI, and 3) guiding users to check how secure a software is before its adoption and use.

**i. Checking data security, functionalities and threats and flaws in the cloud business intelligence**

Participants indicated that a security framework was necessary for enterprises to assess data security, vulnerabilities, risk, and security functionalities in the cloud solutions to be adopted or already in use. Opinions and views of some participants suggested that decision-makers were convinced that when they use a security framework, they might be able to identify security issues within the cloud services before adopting them. Selected extracts support the findings.

Although I have not used a framework, I think it should be used to make sure that the app or system I want to adopt is safe to use particularly those aspects which are not technically capable. The framework should assist us in checking a few things that we want to verify when intending to evaluate applications. **[Participant 5]**

I think we should be able to locate vulnerabilities in the interface, cloud provider, solutions provided, the possibility of data breaches and the magnitude of the damage. It should be user-friendly, devoid of strange technical issues. **[Participant 6]**

I think the framework will make a big difference, particularly if a small business is to be aware of it and be able to use it to assess various cloud services. I think people can figure out how to use the framework to identify security threats in their business environment. Cyberspace is used. It will be easy to look for loopholes to check. **[Participant 8]**

There are always new problems related to security in emerging technologies that small businesses will not be able to cope with without guidelines to assess them. I think a framework with appropriate guidelines is acceptable in our situation. The problem I foresee is whether it will be catering for all businesses. The framework will come as a relief to many small business enterprises. **[Participant 9]**

Although the participants did not have enough knowledge of the frameworks, their narratives revealed that they had the basic functional information about the use of security frameworks which could be important in the proposal and formulation of the framework in this study.

**ii. Making the selection of Cloud BI easy and giving direction on the safe use of the application**

Participants suggested that the use of a security framework would make the selection of Cloud BI an easy process in that they will have a point of reference and directions for safe use of the technology.

I can say that a security framework decides when I can use business intelligence and what sorts of activities to use it for. I want things done easily and effectively, correctly so that I get results quickly. **[Participant 2]**

It should enable us to have an insight into the threats that are not clear. One should know whether the product being used is the right one or not. It should tell us whether the data is safe in the clouds. I am one person who is so particular with safety in IT. I want to do things transparently so that I do not regret them in the end. Even if the security framework is available, I also want to know whether it works according. **[Participant 3]**

I can guess by saying maybe instructions on what to do when assessing different software, explaining how to go about looking for defects and risks in a system before one uses it. I would prefer clear and elaborate guidelines that can be understood by a layman like me. I think guidelines on what security loopholes to look for. If possible, we should be able to locate the hosting computers and the errors in the code. The framework should enable the BI users to check whether what CSP promised is viable. **[Participant 8]**

The extracts show that participants believed that decision-makers would prefer to use the security evaluation frameworks to select the right tools and expect to be guided to use Cloud BI safely in their enterprises. Participants expected to use the framework in various ways that would eventually guide them to select the most appropriate Cloud BI, which would reduce security and financial risks to their business. However, participants were sceptical with the framework as they suggested that they needed to ascertain whether it would provide them with the right solutions.

### **iii. Verifying whether cloud applications meet the security requirements of the enterprise**

Another area in which the participants felt the framework could be of importance was the verification of the security of Cloud BI based on the requirements of the enterprise. Participants were of the view that when they had a security framework, it would be easy to verify whether the security features of the Cloud BI corresponded with the enterprise's expectations. Participants were highly expectant of the framework without giving due consideration to their capabilities of using it.

I can say that a security framework decides when I can use business intelligence and what sorts of activities to use it for. I want things done easily and effectively, correctly so that I get results quickly. **[Participant 2]**

The framework can assist me to check whether there is a link between what the app does and what is expected. Maybe it should guide me in checking whether my data is safe, and no one is accessing it without my permission. I want to be sure that the steps I use when choosing BI are correct and can select the right tool for my organisation. **[Participant 4]**

I think we should use it to get insights into the security situation of the services or applications we want to adopt. It should enable the enterprise to check whether the functionality and security features of the cloud meet the requirements of the organisation it will be used for. I expect the framework to help us to deal with the aspects of the cloud that should be evaluated. **[Participant 9]**

These findings further confirm that participants were aware of the importance of security risk management when adopting new IT solutions. In the QUAN phase, respondents rated the appropriateness of the use of a security framework based on a 3-point Likert scale (*Appropriate = 3; Not sure = 2; Inappropriate = 1*), depicted in Table 4.9. The results reveal that respondents rated each use of a security evaluation framework as being appropriate as indicated by the mean scores of 2.5 to 2.8. At least 73% of the respondents perceived the use of the framework as being appropriate for the evaluation of Cloud BI in SMEs. Respondents believed that SME decision-makers needed guidance in how to manage and run information systems and services in their enterprises, and how to minimise security risks due to exposure of vulnerable Cloud BI to cyber threats.

**Table 4.9: Perceived usefulness of security framework**

| The usefulness of security evaluation framework for Cloud BI   | Ratings of appropriateness (n = 57) |                |                     | Mean | Std. Dev |
|--|-------------------------------------|----------------|---------------------|------|----------|
|  | Appropriate f (%)                   | Not sure f (%) | Inappropriate f (%) |      |          |
| Explains to all parties how information, systems and services are managed within the enterprise  | 46 (80.7)                           | 9 (15.8)       | 2 (3.5)             | 2.8  | 0.5      |
| Reducing risk levels and exposure of an organisation to vulnerabilities  | 42 (73.7)                           | 12 (21.1)      | 3 (5.3)             | 2.7  | 0.6      |
| Instils confidence in an industry or establish a strong reputation with potential business partners and customers                              | 39 (68.4)                           | 13 (22.8)      | 5 (8.8)             | 2.6  | 0.7      |
| Provides a common language and systematic methodology for managing cybersecurity risk  | 40 (70.2)                           | 5 (8.8)        | 12 (21.1)           | 2.5  | 0.8      |
| Provides an enterprise with a chance to identify areas where existing processes may be strengthened, or where new processes can be implemented | 38 (66.7)                           | 9 (15.8)       | 10 (17.5)           | 2.5  | 0.8      |

### **Sub-theme 5.3. Opinions and views on types of framework decision-makers expected**

The opinions of participants emphasised two major characteristics of a security evaluation framework they thought might be of use to SME decision-makers with basic IT skills. Participants expected a framework that; 1) provided simple guidelines on security evaluation that were easy to understand and use without involving IT experts, and 2) was economical in time and proved reliable results.

#### **i. Provision of simple guidelines on security evaluation of cloud business intelligence**

Participants 1 and 4 expressed similar sentiments on the need for a framework with simple checklists and guidelines that is user-friendly for people with little technical knowledge and skills in IT and security in general:

I will prefer a simple tool that does not want me to program while guiding me to check if this and that is working in the cloud. I want a situation where I have something in the form of checklists to fall on whenever I do an assessment. I expect a security evaluation framework to show me what to expect from a good cloud application, ascertain authentication, and access control ... If possible, I would like to know how reliable the cloud application is by looking at the history of other users. **[Participant 1]**

Instead of having sophisticated technical tools for us, why don't they provide simple guidelines or checklists for people like me so that I can use them to assess any IT product available? Although I might not be able to conduct a proper evaluation like an expert, I still need to decide on the security controls to be used and the safety features of the cloud business intelligence in terms of stipulated requirements and the framework that should provide for that. **[Participant 4]**

Although participants did not have much knowledge about the frameworks, their contributions were important as to what should constitute a framework. Participants acknowledged that a framework was essential for providing guidelines to be used by decision-makers when evaluating Cloud BI.

#### **ii. An economical and reliable framework to assess Cloud business intelligence**

Participants expressed that a security evaluation framework should be economic and reliable when used at any stage of its life cycle. The excerpts from participants 5, 9 and 11 indicate that decision-makers were worried about the costs of using a security framework and the reliability of the results. This indicates that they expected a framework that should provide them with credible guidelines in selecting the most appropriate Cloud BI without compromising their financial positions and standing. For example, **Participant 5** asserted,

I do not want to use an expensive and time-demanding tool that gives me results that will not assist in making the business viable. ... at times something new comes in and then within a few weeks it has been changed so many times before one has implemented the first results. It becomes a waste of time and resources to use such a tool. I expect something which lasts a long time and provides clear and meaningful results that I can use to decide whether to adopt Cloud BI or not. I do not have that kind of money to keep trying out things that do not work.

**Participant 9** was of the view that a framework should not be expensive in terms of time, energy, and financial resources required to identify issues within an application being evaluated if it is to be of use to struggling SMEs.

I find it disturbing at times that a tool is praised so much and then when you try to use it, you will have to take a course that is difficult for some of us. It is uneconomical of no business, a value to spend a lot of time trying to learn and understand a framework that leads you nowhere at all. I want a framework that is communicative and gives clear direction without using much of the scarce financial resources. These days it is easy to hide behind IT jargon or sound so big when the opposite is true. A framework that seeks to encourage the use of technology should be free and elaborate.

Another participant was of the view that regardless of the technology being used, there should be many considerations when it comes to evaluation tools used by SMEs who struggle financially and lack technological know-how in evaluating emerging IT solutions. The participants argued that SMEs needed to be protected from CSPs by having a standardised way of evaluating Cloud BI.

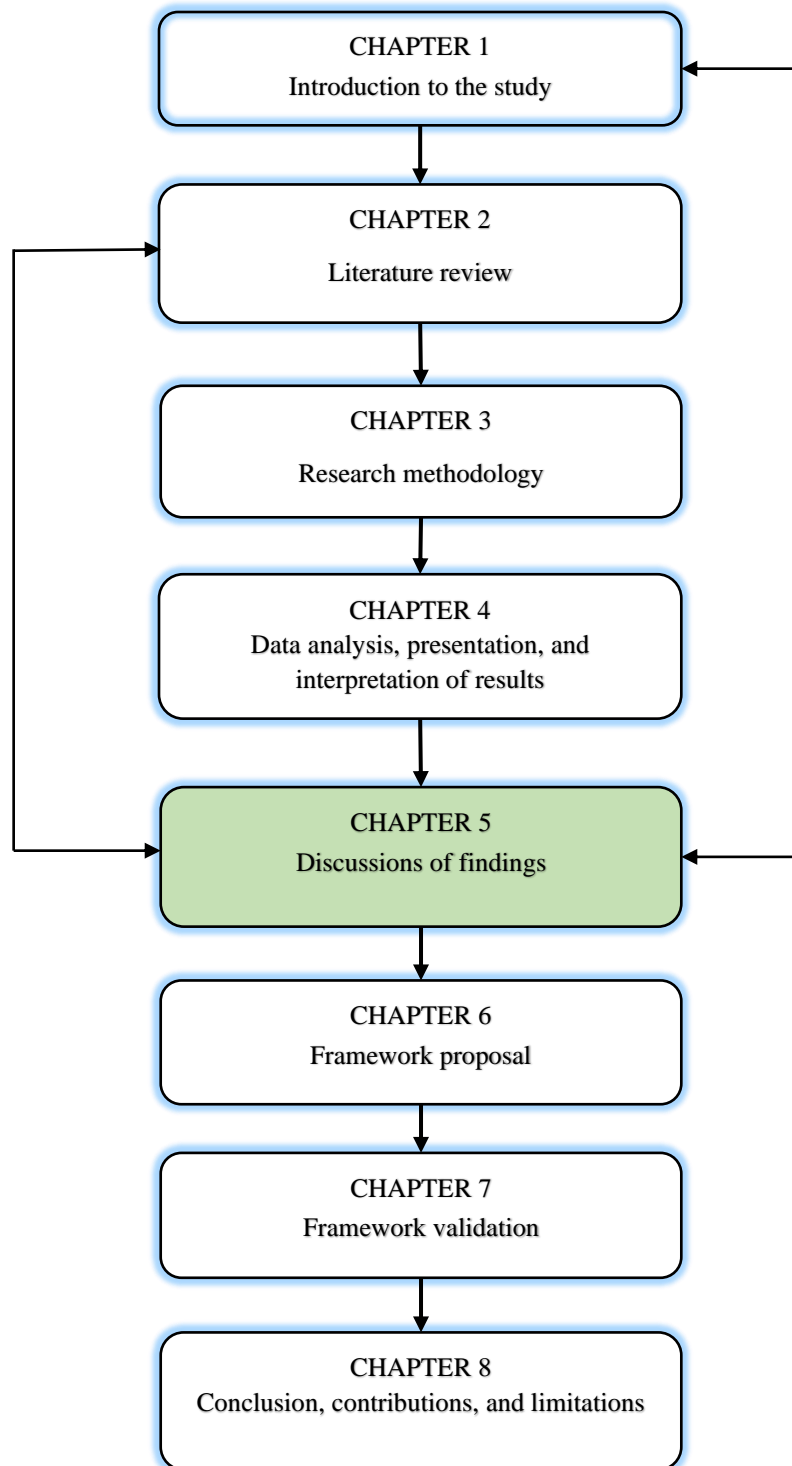
There are many cloud service providers today and will even be more tomorrow. These entities will always differ even if they were to offer the same cloud solution. One will claim to be the best even if they are not doing the right thing. This is why a simple framework should be made available to enable us to evaluate and decide which is which without being subjected to a laborious technical process we are not familiar with. No business person would want to select a difficult tool that requires a lot of financial resources and time to use them. I prefer a tool that requires very little in terms of effort and money but gives me the best output. **[Participant 11]**

These statements show that decision-makers expected to have a security framework that was both economical and reliable to reduce financial burden and risk. Decision-makers in SMEs take more time to act as they weigh many factors and, in some cases, may lack relevant information to arrive at the correct decisions.

## **4.2. Conclusion**

This chapter presented findings from the QUAL phase which were integrated with the results from the QUAN phase during analysis and interpretation. The findings included the efforts made by decision-makers and challenges faced in the adoption and use of Cloud BI by SMEs. Decision-makers have functional knowledge about the security evaluation process, the considerations made, and the challenges it poses to the adoption of Cloud BI in the Province. The adoption of Cloud BI

by SMEs was very low as most of the enterprises were at the awareness, interest, and evaluation stages. There was enough evidence from the findings that decision-makers were familiar with the use of checklists, guidelines, and policies in the evaluation of IT solutions, although they were not able to use the tools effectively or regularly. SME decision-makers face security evaluation challenges, such as limited knowledge and skills, lack of available information during evaluation, and ignorance of which evaluation tools to use. Decision-makers found it difficult to use traditional and industry security evaluation tools as they had limited security knowledge and skills needed. Discussions of findings are presented in the next chapter.



## **5.1. Introduction**

The previous chapter presented and analysed the results for both the QUAL and QUAN phases of the study. This chapter discusses the findings of the study based on the four sub-research questions formulated in Chapter 1 and explored in the other chapters of the study. The remainder of the chapter is organised into two major sections, namely discussions of findings and summary of the chapter.

## **5.2. Discussion of findings**

This section discusses the findings of this study based on the sub-research questions supported by literature from the previous chapters. The four research questions the findings apply to are:

*SRQ1: What factors influence the adoption and use of Cloud BI among SMEs in small South African towns?*

*SRQ2: How do small and medium enterprise decision-makers evaluate Cloud BI before adoption?*

*SRQ3: What challenges do small and medium enterprise decision-makers face when evaluating Cloud BI?*

*SRQ4: What do decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises?*

### **5.2.1. Characteristics of decision-makers and the enterprises**

Literature in technology adoption reports the importance of demographic information as a determinant of the adoption process (Berkowsky et al. 2017). Therefore, demographic information was important in highlighting the types of enterprises and characteristics of decision-makers who took part in this study. The majority, 83.4% of the respondents, who were likely to recommend the adoption and use of Cloud BI, was in SMEs situated within towns compared to those from peripheral locations. This is consistent with Geer and Sullivan (2019) who purport that the location of an enterprise is an essential factor in the adoption of IT due to multiple information sharing channels about technology innovation among enterprises. The findings illustrate that decision-makers from SMEs, with good networking among themselves, had higher chances of successfully adopting emerging technologies as they get more information and encouragement from their peers.



Such good networks are found among SMEs which are close to each other and are likely to be located within towns.

In terms of decision-making, 63.2% were owners of small enterprises and 36.8% were family-appointed managers of medium enterprises. Several studies emphasise the importance of SME owners in the decision-making process (Hashim & Hassan 2015; Mashandudze & Dwolatzky 2015; Salim et al. 2015). According to Salim et al. (2015), SME owners usually form positive perceptions about technology adoption as their knowledge increases with awareness of the trial stage. In this regard, owners become more influential in decision-making than family-appointed managers. With a larger percentage of owners taking part in the study, the findings were closer to the experiences and knowledge of the targeted group of decision-makers in SMEs in the Limpopo Province.

There was a gender imbalance among SME decision-makers, with 68.4% being male and the minority, 31.6%, were female decision-makers. The finding was consistent with that of Boonsiritomachai, McGrath and Burgess (2014) showing 60% of male to 40% of female decision-makers actively using IT solutions in managing enterprises at Thai SMEs. The ages of the decision-makers ranged from 30 to 60, with most of them, 65.0%, in the age range 41 to 50 years, thus middle-aged individuals who could be inclined to recommend the use of emerging technology, depending on benefits and risks. Age is one of the widely used demographic characteristics in technology acceptance studies (Berkowsky et al. 2017; Opara-Martins et al. 2016; Niehaves & Plattfaut 2014). Studies on technology adoption have found that elderly individuals are reluctant to adopt and use new technologies due to their poor perceptions of benefits and knowledge (Berkowsky et al. 2017; Niehaves & Plattfaut 2014; Jansen, Curşeu, Vermeulen, Geurts & Gibcus 2013). Contrary, this study established that most of the decision-makers had a fairly good knowledge of the benefits that can be derived from using Cloud BI and other technologies, although they had not adopted them.

The educational qualifications of decision-makers were mainly diplomas, 73.7%, generally perceived as a good educational level in South Africa, which may have a positive impact on the use of ITs to support business operations among SMEs. In terms of experience in IT usage, 66.7%

of the decision-makers had been using IT systems to support their businesses for 4 to 6 years. Thus, a good educational qualification coupled with good experience in using on-premise IT applications, and knowledge of the benefits of using Cloud BI placed the decision-makers at an advantage in evaluating these applications.

On the state of IT facilities in the SMEs, 66.7% of the decision-makers perceived it as good enough to support business operations. This was inconsistent with findings made in some previous research studies that report poor IT facilities among SMEs as the major cause for poor uptake of cloud computing technologies (Mohlameane & Ruxwana 2014; Lacey & James 2010). For SMEs to adopt and use Cloud BI, they need not have advanced IT facilities (Papachristodoulou et al. 2017; Boonsiritomachai et al. 2014), because they are hosted by CSPs somewhere else (Fernandes et al. 2014). This tells us that SMEs in the selected small towns had enough IT facilities to support the adoption of Cloud BI.

The duration of awareness of Cloud BI among the decision-makers ranged between 1 and 6 years, with the majority, 70.1%, having at least 2 years, a mean score of 2.6 (SD = 0.9). This indicated that awareness and knowledge of Cloud BI and other cloud services had permeated SMEs using various IT systems in the province. This was a welcome development in contrast to traditional BI which was poorly received among SMEs (Mashandudze & Dwolatzky 2015; Thompson & van der Walt 2010; Wailgum 2010). Although awareness of Cloud BI among decision-makers was an important factor, it did not explain their experiences and skills in the use of technology, only its existence. It would seem that decision-makers still required advice and solutions, such as simple guidelines, from relatively low-cost policy and awareness measures to advanced IT solutions that need IT specialist advice (Rostek et al. 2012; Lacey & James 2010).

The technology adoption styles of decision-makers were found to be mainly: the early majority (21.1%), late majority (42.1%), and laggards (28.0%). This finding was consistent with Rogers' (2005) categorisation of technology adoption based on the DoIT for business use in contrast to individual use. This implied that decision-makers were still hesitant to adopt Cloud BI due to the challenges discussed in subsequent chapters. The majority of the enterprises (57.9%) preferred to

access Cloud BI over the secured web, indicating that they were aware of the security issues involved.

### **5.2.2. Factors influencing the adoption and use of Cloud BI among SMEs in small South African towns**

The finding was that the level of adoption and use of Cloud BI by SMEs in the five selected towns were low even though most of the decision-makers (70.2%) indicated having good knowledge about the benefits of the uses of Cloud BI in data management and decision-making. According to Ettlie and Penner-Hahn (1994), the knowledge of the availability of new technology by enterprises was a positive step in the evaluation stage. Researchers who emphasise the importance of knowledge on innovation adoption include Rogers (2005), Lai (2017), and Fry, Ryley and Thring (2018). With good awareness of the benefits of Cloud BI among decision-makers, it was expected that the adoption could have been appreciably higher than the current level. These findings were consistent with those in previous studies on the benefits of adopting and using cloud services (Ukil, Jana & Sarkar 2013; Labes et al. 2012). Several models of the technology adoption process regard the perceived benefits of the technology as an important aspect that adopters consider before they adopt and use any technology (Nyoro et al. 2015; Hashizume et al. 2013). TPB and TAM regard this as the perceived usefulness of technology (Ajibade, 2018; Tamer, Kiley, Ashrafi, & Kuilboer, 2013). Most of the benefits investigated were found to arouse the willingness of the decision-makers to evaluate Cloud BI but did not result in meaningful adoption. This was worth noting, that SMEs were not “blinded” by benefits only but had other underlying issues with the cloud that could subsequently affect the business operation when they started using Cloud BI.

The cloud was perceived as an unsafe environment for SMEs to operate in by 61.4% of the respondents and this was thought to have a big influence on decision-makers to adopt and use Cloud BI. The findings show that decision-makers were not sure about the security status of various cloud deployments and were quick to express their doubts on this benefit. There are reports of cyberattacks on the public domain that reinforce the perception that the cloud is an unsafe environment (Patil & Chavan 2020; Alia et al. 2015; Fernandes et al. 2014). The poor adoption of Cloud BI in the province was confirmed by the stages of adoption at which most SMEs were, in which 40% were still at the interest stage and 28% struggling at the evaluation stage, very few

were at the trial stage of adoption. Those who purported to have adopted Cloud BI were not using the technology meaningfully for business purposes, but parallel with traditional IT systems. The interest and willingness to use the technology were dampened by the belief that the evaluation process was very difficult for decision-makers to perform. A study by Boonsiritomachai, McGrath, & Burgess (2014) of SMEs' adoption and use of BI in Thailand found that the willingness to adopt did not translate to meaningful uptake of the technology due to negative militating factors. Similarly, Salim, Sedera, Sawang and Alarifi (2014) found that the evaluation, as well as the trial stages, are critical in the technology adoption process as they required decision-makers to put more effort into assessing each available cloud service they were interested in. Unlike previous studies, Mohlameane and Ruxwana (2013, 2014), which associate the low uptake of cloud services by SMEs to a lack of knowledge of the different Cloud BI solutions available, this study has established that this awareness has greatly improved and other challenges were the main drawbacks.

Implicitly, the enthusiasm and willingness to adopt and use Cloud BI by decision-makers were based on the perceived usefulness of Cloud BI, a finding made in previous research (Taherdoost 2018; Ghobakhloo et al. 2011). This study established that decision-makers were not prepared to make hasty decisions without insights into security issues in Cloud BI and the how-to-knowledge needed to select and use the technology meaningfully. This emphasises the importance of different forms of knowledge that decision-makers need to have, particularly the “how- knowledge and principles-knowledge” (Osborn 2014; Sahin 2006; Rogers 2005). These decisions could have been based on decision-makers' experience with IT technologies currently in use and their lack of concrete Cloud BI technologies available due to the proliferation of such technologies (Ren 2019; Senarathna et al. 2016; Moore 2014). Although the benefits of Cloud BI were appealing to lure decision-makers to adopt and use the technologies, challenges were preventing the SMEs from adopting the technology.

### **5.2.3. Evaluation of cloud business intelligence by small and medium enterprises before adoption**

The findings for this research questions were based on how decision-makers perceived Cloud BI or how any other cloud services could be evaluated and what they considered to be essential during

the evaluation process. The how-to-knowledge was examined to determine whether decision-makers systematically evaluated Cloud BI and the various areas they evaluated. The findings of this research question are discussed under three categories, namely, the evaluation process; the major considerations made during the evaluation process; and challenges faced during the evaluation process.

### **Steps taken by decision-makers when evaluating cloud service applications**

Although the state of adoption of Cloud BI among SMEs was low, the study found that enterprises at the evaluation stage were engaged in different evaluation activities that could eventually be useful to the decision-makers to adopt Cloud BI or not. Findings from both phases show what decision-makers perceived as security evaluation in Cloud BI, how they conducted the process, and the tools they believed should be used. The findings were that decision-makers perceived security evaluation in Cloud BI as involving:

- the identification of appropriate Cloud BI and gathering relevant information about threats and flaws in the application from various sources including the web;
- the identification of a CSP and checking the history of security, reputation, and trust contracts in Cloud BI;
- the use of free or trial applications to assess functionality for access control, data security issues and portability of the application;
- the use of existing guidelines and checklists to evaluate Cloud BI;
- assessing the level of skills and knowledge needed to operate or use the Cloud BI app;
- assessing the level of data control in Cloud BI that the user and CSP will have;
- assessing physical security of data centres as well as their computer systems; and
- assessing the business value and financial risks associated with Cloud BI use.

The findings show that decision-makers did not follow a systematic way of evaluation but only identified critical activities they perceived should be undertaken in a proper evaluation. Furthermore, there was no distinction between the evaluation and trial stages as previously observed in the Multi-Stage Adoption Model (Ettlie,1994).

**i. Identifying Cloud BI and gathering relevant information about threats and flaws in the application from the web and other sources**

All 13 decision-makers interviewed were elaborate on the need to identify different Cloud BI from the web and other sources and then search for relevant information about vulnerabilities, threats, and functionalities relevant to business operations. Decision-makers believed that they needed current and correct information on security vulnerabilities and threats for each identified Cloud BI and CSP. This highlights that decision-makers were aware of different sources of information, such as websites of security organisations, IT reports, blogs, IT specialists, friends, and competitors. The QUAN findings confirm that 80.7% of the respondents preferred to use critical historical and current information about the frequency of cloud service unavailability to the users as a means of evaluation criterion. A rating of the mean score of 3.9 (SD = 1.2) by 73.7% of decision-makers indicates a very strong affirmation that they would check for reported cases of unanticipated alterations to data or information that occurred in CSPs, and the risk management strategies implemented to solve the problem. Decision-makers were convinced that the benefits and flaws of popular cloud deployment models and services were documented, and such information could be located and used for evaluation purposes. It could be argued that decision-makers valued current and historical information about Cloud BI from credible sources, such as security organisation websites, friends who use the system, and IT specialists.

Information search is critical in the technology adoption process and has been in use for a long time (Salim et al. 2016; Ettlie & Penner-Hahn 1994). With an abundance of information about technology in the public domain, individuals are encouraged to rely on various sources such as enterprise networks, the web, and specialists to obtain, verify and process the information on new and complex technologies (World Economic and Social Survey 2018). This observation emphasised the need for social learning among decision-makers which can influence technology adoption in SMEs in the long run (Alshamaila et al. 2013). Several studies acknowledge the role played by networks in reducing the social distances between individuals, households and firms and the easy spread of information about new technologies (World Economic and Social Survey 2018). However, the spread of information may not translate to the useful knowledge needed to aid the adoption of the technologies due to barriers in the information itself and the complexities of technologies.

There are many sources of information about Cloud BI on the web, which decision-makers should identify, evaluate, and use to select the right application. However, the multitude of sources available may be overwhelming and confusing for decision-makers on an already busy schedule and who may lack the necessary information literacy skills to handle such large volumes of information. Furthermore, some of the information may be specific to certain business models and not useful to others. Although consulting friends is a good idea, it has its limitations, such as biases, being unscientific, and being limited in-depth regarding key security issues to evaluate. Information shared between friends may not reach other clients outside of the network, thereby delaying the evaluation process (World Economic and Social Survey 2018). SMEs in different economic sectors need different types of information for their business activities. Decision-makers who need specific information might not benefit from networking with colleagues in different economic sectors. Another important factor is that enterprises vary in their operations and the data they generate present different business opportunities to scammers and hackers and the type of security threats would differ. Therefore, information needs vary in vulnerabilities and threats to the business operations of each economic sphere.

**ii. Examining the CSP history of security, reputation, and trust in contracts**

This finding indicates that the CSP history in security, reputation, and trust in service provision (contracts) concerning business value is important for decision-makers to justify whether to subscribe to a CSP or not. Decision-makers believed that by looking at the history of CSPs, they would learn how reliable providers were. Decision-makers were of the view that reputable CSPs had a well-documented history of secure applications and were trusted by many SMEs. Decision-makers were certain that reliable information from various security organisations or publications about the CSPs could be used to successfully assess the providers' history in security, reputation, and trust. Most of the decision-makers, 80.7%, confirm their preparedness to request CSPs' reports on periods of downtime of services to the users and measures taken to avert operational disruptions in the future. The inference drawn from these findings was that SMEs were no longer ordinary consumers of any technology given to them but were prepared to evaluate it.

There is a growing number of studies on cloud computing that emphasise the need for clients to verify the security history, reputation, and trust of CSPs during the evaluation process (Perkins 2016; Huang & Nicol 2013). A study by Huang and Nicol (2013) encourages clients to choose CSPs based on their reputation and trust in providing security and adhering to contracts. Similarly, Edwards (2009) advises potential cloud clients to demand transparency by making sure that the CSPs provide them with detailed information on the security architecture and an undertaking to accept regular security audits. Edwards (2009) further emphasises that clients should request specific information about user control from CSPs, particularly the hiring of new employees and supervising privileged administrators and controls over their access to information and data in the cloud. Huang and Nicol (2013) acknowledge that trust and reputation are different but related in that for an entity to be trusted, it must have a high reputation of many entities in that community. Edwards (2009) encourages potential cloud clients to request specific information on user access, regulatory compliance, and data location from CSPs. Greis (2014) posits that for a cloud to be secure, it should have appropriate controls for protecting the CIA of the applications, information and data that are stored in it. Greis (2014) also highlights the needs for the CSP to put the right procedural and technical protections in place to protect data at rest, in transit, and in use.

Trust between enterprises and CSPs was found to be very important, and this encouraged the enterprise to examine the CSPs' history in security, trust, and contracts because of the business value of Cloud BI to the enterprise. The majority, 87.7% of the decision-makers, preferred verifying whether the expected operational and security functionalities and results of Cloud BI matched the claims made by CSPs. Most of the decision-makers, 84.2%, concurred that decision-makers should check for any possibility of employees of CSPs having access to manipulate enterprise data without permission when evaluating Cloud BI. The implication is that decision-makers know the importance of contracts undertaken when subscribing to CSPs. The majority, 91.2% of the decision-makers, emphasise the need to avoid being tricked into signing contracts with poorly performing CSPs after the evaluation of Cloud BI. The need to be cautious about the contracts and SLAs compelled decision-makers to resort to the history of the CSPs during the evaluation stage. The majority 80.6% of the respondents agreed that the evaluation process should involve identifying all possible sources of conflict they might have with the CSP about SLAs before they enter into any agreement.



The literature on the assessment of cloud services shows that enterprises value the trust associated with the service more than anything else (Kodagali 2019; Alshamaila et al. 2013). According to Kodagali (2019), the most common reason for rejecting a cloud service by an enterprise was the lack of trust. Similarly, Kerravala (2019) warns clients of the differences between SLAs and reliability which can be measured by downtime. In this context, decision-makers should be aware of the cunning nature of CSPs who promise 100% SLAs but might not be able to reimburse clients for business lost due to service unavailability. Some CSPs are reported to be unforthcoming in consistently disclosing service disruptions but tend to confuse the clients with meaningless solutions (Kerravala 2019; Yu et al. 2017).

There are many popular CSPs from which SMEs can choose (Mashandudze & Dwolatzky 2015). Choosing Cloud BI and CSPs based on reputation is helpful with the first provider and becomes ineffective with subsequent choices, especially when the client has gained enough knowledge and skills and the demand for performance and reliability increases (Huang & Nicol 2013; Pearson & Benameur 2011). Reputable CSPs such as Amazon Cloud, IBM, GitLab, Facebook, Amazon Web Services, Microsoft Azure and Microsoft Office suffered credibility and reliability due to cloud service failure between 2013 and 2018, which affected services available to the clients (Mesbahi et al. 2018). Other criteria for evaluating CSPs and Cloud BI need to be considered to complement the history and reputation of CSPs.

According to EY (2014) and Werff et al. (2019), a trusted cloud environment should provide high availability of data by being resilient and withstanding adverse conditions and threat events. EY (2014) and Mogull, Arlen and Gilbert (2017) advise enterprises to use an audit-ready cloud ecosystem, which has continuous compliance supported by a certification that meets specific industry regulations, legislation, and easily verifiable compliance. Enterprises need to assess the past performance of the CSPs using information about known breaches, malicious use of cloud services, and the penetration testing conducted by the providers (Kodagali 2019; Mogull et al. 2017; Perkins 2016). Thorough background checks of CSPs have become important (Mashandudze & Dwolatzky 2015; Edwards 2009). The Cloud Standards Customer Council

(2017) encourages clients to check whether CSPs have the right and relevant certifications in place, which proves compliance with industry standards or regulatory requirements.

**iii. Using free or trial applications to assess authentication, authorisation, and data security issues associated with the applications**

The use of free and trial Cloud BI was found to be crucial in the evaluation process. Decision-makers adopted a pragmatic hands-on approach when evaluating IT solutions and this served dual purposes, namely, checking the security features that CSPs purport to be in the application; and familiarising with the features and functionalities of the system.

The findings suggest that decision-makers used free and trial versions not only to learn how the applications worked but to identify weaknesses and threats in them. Decision-makers confirmed their readiness to assess information asset accessibility to the public by unauthorised cloud users. Furthermore, decision-makers were eager to check how easy it was for outsiders to manipulate data processing on clouds using reported cases of unexpected changes to data or information that would have occurred in the cloud. To achieve this, there was a suggestion for the use of the trial version during the evaluation process.

The use of a trial version or limited versions is a common practice encouraged in the IT industry for the potential user to familiarise themselves with the solution and check whether it meets business needs (Salim et al. 2015; Khorshed et al. 2012). The purpose of using a trial version is to afford clients a chance to gather as much information about the application which is then used to make decisions about the security features of interfaces for user access control of the system and compare them to those found in stand-alone systems (Werff et al. 2019; Constantinides et al. 2012). A trial version can be used to check whether data can be accessed by unauthorised users when being migrated to the cloud. Sahandi, Alkhalil and Opara-Martins (2012) suggest that decision-makers should check if it was easy for attackers to get passwords, access, or inspect and modify or delete data being transferred or stored in the cloud. Some studies emphasise that decision-makers must check that the application implemented a reliable safe authentication process, encrypted procedures, and secure backup applications (Hurtaud, de la Vaissière & Aboukir 2017; Sahandi et al. 2012). A report by Kodagali (2019) on the assessment of cloud services, indicates

that enterprises who requested information about the services wanted to be assured of authentication and identification. The security attributes that enterprises sought in the cloud included multi-factor authentication, anonymous use, identity federation method, and enterprise identity (Kodagali 2019). Due to the newness and dynamic nature of cloud services and applications, the assessment of these attributes is reported to be difficult, something that decision-makers in this study have confirmed.

#### **iv. Using existing checklists and guidelines to evaluate Cloud business intelligence**

The use of guidelines and checklists as tools in the evaluation of Cloud BI was found to be a common practice inherited from traditional IT solutions. This finding indicates that most of the decision-makers, 66%, were familiar with the use of guidelines and checklists in evaluating IT solutions. Decision-makers believe that when given the right evaluation guidelines and checklists, they can evaluate any application. Very few respondents, 35%, indicated that decision-makers were familiar with the use of models and frameworks in evaluating applications. Although decision-makers were prepared to use guidelines and checklists to evaluate Cloud BI, they were not certain of which one to use and where to find these tools.

There is a plethora of literature discussing the tools and methodologies used in evaluating traditional IT applications but they do not give references to Cloud BI in particular. Dyczkowski, Korczak and Dudycz (2014) argue that although there were many models and frameworks for evaluating BI, there was a lack of guidelines and checklists informing how to create and evaluate BI that could be used as reference examples by SMEs. Choi and Lee (2015) argue that guidelines and checklists are among the most common evaluation tools that can be useful to SMEs in evaluating cloud services because they are easy to use. Perkins (2016) posits that guidelines are useful in assisting decision-makers in interpreting and implementing specific policy requirements. Gleeson and Walden (2014) assert that NIST provides guidelines for addressing fundamental issues in cloud security and privacy including architecture, identity and access management, trust, software isolation, data protection, compliance, availability, and incident response. SMEs' decision-makers are either not familiar with the industrial standards such as NIST, COBIT, and ISO 27001 or find them difficult to implement. The literature underscores the importance of cloud including SMEs to understand data security, standards and procedures and technical infrastructure security about the cloud service they intend to use (Widyastuti & Irwansyah 2018; Yu et al. 2017;

Shimamoto 2015). According to Antoo et al. (2015), SMEs need to have insights into the evaluation of Cloud BI based on security flaws, cyber threats, and risks in internal network controls, data storage, and CSPs' SLAs with regards to their requirements and security policies.

**v. Examining the level of knowledge and skills needed to operate or use the Cloud business intelligence.**

This finding confirmed the importance of assessing whether the application was easy to use without undergoing special training or workshops. A mean score rating of 3.9 (SD = 0.6) by 76.4% of the decision-makers was an indication that the need to assess the level of skill required to operate or use the Cloud BI was an important evaluation criterion that should be used.

The perceived ease-of-use (PEU) is viewed as important when evaluating Cloud BI to avoid applications that required the users to have formal training to use it. Technology adoption theories such as TPB, TAM, and other studies have explored the concept of PEU and found it central to the adoption of IT, including cloud computing technologies (Lai 2017; Olushola & Abiola 2017; Bach et al. 2016). PEU was found to have a strong influence on initial decisions to adopt innovation or technology among adopters with a low level of knowledge and skills, particularly owners and managers of SMEs (Taherdoost 2018; Olushola & Abiola 2017). With Cloud BI, tutorials are available in slides and videos to demonstrate how easy it is to learn and to use the application. The level of knowledge and skills needed to operate the application is an important area to evaluate IT solutions.

Decision-makers preferred Cloud BI which required little time and effort to learn to operate over those which demanded more of their time and effort. The preference for easy-to-learn and easy-to-use Cloud BI was because decision-makers were afraid of making mistakes that would risk their chances of making profits. Decision-makers were obliged to assess how difficult it was to learn and use Cloud BI because they believed that an easy to learn and use Cloud BI could lead to fewer security breaches by users compared to a difficult one. Literature shows that the poor adoption and use of traditional BI by SMEs was due to the high level of knowledge and technical skills required to operate the application (Llave 2019; Ramachandran & Chang 2016; Mashandudze & Dwolatzky 2015). Decision-makers are cautious of adopting Cloud BI with little how-to-knowledge and

principle-knowledge needed in the successful utilisation of the technology. This finding emphasises the need for decision-makers to know of the existence of various Cloud BI, how they work, how to use them, the outcomes in terms of business benefits, and the security risks involved.

**vi. Assessing the level of access to data and control in Cloud BI that the user and CSP have**

The level of data control by CSPs was found to be an important area that most of the decision-makers perceived should be evaluated. The fear of losing data control to CSP and unauthorised access by CSPs' employees convinced decision-makers to emphasise the need to assess this security issue before deciding to adopt and use the application. Decision-makers were afraid of CSPs having total control over their data which they could use for malicious intent, such as ransom, signing expensive contracts, and even mining for competitors. Decision-makers want to remain in control of their data and applications in the cloud and need to restrict CSPs' influence. This was supported by 82.4% of the respondents (mean score 4.2; SD = 0.3) who affirmed the necessity for verifying whether the enterprise could migrate its data to other CSPs easily. Close to 81% of the respondents advocated for the assessment of the level of control of data in the cloud that the enterprise would have.

This finding shows the willingness of decision-makers to assess the level of access to data and control CSP have and the extent to which their employees were able to access the same data. Literature shows that enterprises are always concerned with the security of their data because they cannot see who gains access to these files and fear that their sensitive information may end up in the hands of malicious users (Amigorena 2019; Vasista 2015). CSPs face serious challenges in stopping their employees from stealing clients' sensitive files before they leave employment (Amigorena 2019; Mashandudze & Dwolatzky 2015).

**vii. Assessing physical security of data centres**

The state of physical security of data centres was another area that decision-makers suggested should be assessed. Decision-makers expressed the desire to visit CSPs' data centres to assess the security of infrastructure to natural disasters, burglary, and unauthorised access. The finding indicates that decision-makers perceived physical inspection as another appropriate way of

assessing security in Cloud BI. A mean score of 4.1 (SD = 0.8) by 73.4% of the decision-makers indicated that inspecting data centres was perceived as an important step in the security evaluation of CSPs. The need to evaluate the security of physical infrastructure was an indication that decision-makers were suspicious of some of the CSPs being unable to provide enough security to their data.

According to the Cloud Security White Paper (2011), potential users of cloud services need to have clear insights into the evaluation of the physical infrastructure in data centres, applications hosted by CSPs that manage clients' data, and the policies and procedures used to continuously maintain security in the cloud environment. According to Sahandi, Alkhalil and Opara-martins (2012), the assessment of the physical location of data centres is important because these are affected by the laws that regulate the management of data in that region. Tashi and Ghernaoui-Hide (2019) posit that security controls can be relied upon to protect IT infrastructures if their operations are clear, and the clients are able to verify them. The internal controls for data centre protections are among the attributes of the cloud deployment that enterprises require from CSPs (Kodagali 2019; Mahajan & Sharma 2015). Although the need to inspect the data centres is important, this expectation showed a lack of knowledge about how CSPs work among decision-makers. With data centres located over multiple sites or different regions, their physical inspection presents a challenge to decision-makers in locating and accessing these facilities.

#### **viii. Assessing the possible financial benefits and risks of using the application**

The study found that decision-makers suggested assessment of financial benefits and risks emanating from the use of Cloud BI as being an important part of the security evaluation process that should be undertaken. This implies that decision-makers looked at the benefits to the business that Cloud BI was likely to bring about without compromising the operations and profits. An increase in cybercrime and possible unethical practices by CSPs and their employees were some of the concerns that compelled decision-makers to consider evaluating financial benefits and risks in the clouds. Close to 65% of the respondents and a mean rating of 3.1 (SD ± 0,6) emphasised the importance of verifying financial gains for the SMEs against risks before recommending the adoption and use of any cloud technologies. To achieve this, decision-makers indicated the importance of seeking security assurance from the CSPs as much as possible. Most of the decision-

makers, 78.9%, with a mean score of 3.1 (SD= 0.7), indicated the importance of considering the assessment of legal and administrative issues which can lead to financial risks. Nearly 82.3% of the respondents, mean score of 3.1 (SD = 0.9), rated vendor or service provider reliability as an important area to examine during the evaluation of cloud services and then to use the information for decision-making whether to adopt. Reliability was important in determining the extent to which the CSP will keep connectivity uninterrupted and being transparent to subscribers. The mean score rating of 3.0 (SD = 0.7) by 80.7% of decision-makers show how important it was to evaluate the compliance of CSPs with national and international legislations. Non-compliant CSPs risked being fined and this would cascade down to their clients suffering financial loss or tarnishing of their reputation. A CSP's compliance certifications are important internal security controls that enterprises are encouraged to request when evaluating cloud services (Kodagali 2019; Information Security Forum 2016; da Silva, da Silva, Rodrigues, Nascimento & Garcia 2013).

The mean score of 2.9 (SD = 0.8) by 77.2% of decision-makers indicated that the fear of financial risks was perceived as a motivator for decision-makers to examine their new responsibilities and liabilities after adopting Cloud BI. The findings show that regardless of the magnitude of financial benefits, the slightest financial risks likely to be incurred would deter decision-makers from recommending the adoption of Cloud BI.

Existing literature discusses the causes of financial risks that enterprises can suffer when they adopt and use Cloud BI, namely hidden running costs, disruption of operations due to unavailability or connectivity issues, and litigation (Gadia 2018; da Silva et al. 2013). Hidden running costs were likely to emanate from the malpractice of CSPs who do not reveal the extra charges to the subscription costs. Such costs are not stated in the contracts and SLAs (Romes 2015). These could be penalties for the improper use of the applications, overcharging of additional services, and services that clients can request.

### **Challenges during the evaluation of cloud business applications faced by decision-makers**

This section discusses the three major challenges which were faced by decision-makers when they were evaluating Cloud BI namely: lack of knowledge and skills to evaluate Cloud BI by decision-makers; lack of appropriate tools to use in the evaluation of the Cloud BI by SMEs; and difficulties

in getting relevant information from the CSPs about the Cloud BI. A brief discussion of each challenge is given in a separate sub-section.

**i. Lack of knowledge and skills needed to evaluate Cloud business intelligence by decision-makers**

Despite having good knowledge of Cloud BI and its benefits, decision-makers were found to have poor knowledge of different types of Cloud BI in the market and they lacked evaluation skills and knowledge to select the most appropriate application for their business needs. Decision-makers felt that without proper knowledge of different Cloud BI and how they worked, it was a challenge to evaluate the Cloud BI. To conduct a meaningful evaluation, the decision-maker should have basic knowledge of Cloud BI and how these applications function. This was compounded by their perception that they lacked technical know-how in evaluating security in IT solutions and CSPs.

In the QUAN phase, the mean score ratings on a 4-point Likert scale support the view that decision-makers' perceived lack of knowledge of Cloud BI and how they work, as well as their poor knowledge to evaluate IT solutions, CSPs and their physical environment are serious challenges. The mean score of 3.6 (SD = 0.4) by 96% of decision-makers showed that the inability to assess vulnerabilities in the cloud, where the BI application would be deployed, was viewed as a severe challenge for decision-makers. Besides, most of the decision-makers, 87.7%, perceived ignorance of flaws in the interface of BI applications as a challenge (mean score 3.4 and SD = 0.8). Another serious challenge as indicated by a mean score of 3.3 (SD = 0.6) by 85.9% of decision-makers, was the lack of skills in the use of existing evaluation tools. Although decision-makers were eager to assess financial liabilities of security breaches and risks, 75.4% viewed their lack of skills and knowledge in this area as a serious challenge, a mean score of 3.3 (SD = 0.9). The finding indicates that decision-makers were worried about their lack of knowledge and skills when using existing tools to evaluate Cloud BI.

SLAs and policies are important documents that decision-makers need to understand to effectively evaluate Cloud BI (Romes 2015). However, 71.4% of the decision-makers indicated that they have serious challenges in understanding SLAs from providers as shown by a mean score of 3.1 (SD = 0.8). The mean score of 3.7 (SD = 0.9) by 91.2% of the decision-makers, highlighted the



seriousness of their lack of skills to evaluate the physical security of provider infrastructure. There is relatively little scholarly literature on the evaluation of Cloud BI by SMEs and how these affect the adoption of Cloud BI. However, the existing scarce literature shows that knowledge gaps in BI contribute significantly to missed opportunities in the adoption of Cloud BI among many enterprises (Evelson & Bennett 2017). According to Kumar (2018), carelessness, lack of knowledge, hurried operations, and unskilled resources are challenges that potential cloud service adopters face.

Challenges faced by decision-makers usually lead to time-wasting when assessing a single solution or CSPs thereby delaying the adoption and use of the technology. Due to the rapid changes in cloud computing technology, decision-makers have very limited time to learn how the technology works and to evaluate its features and the environment in which it is used. These findings confirm that knowledge of Cloud BI and how they operate was essential in evaluating the applications. The finding is consistent with Rogers' (2005) categorisation of adopters, in which the late majority spend most of the time scrutinising the innovation, resulting in them missing out on potential benefits. The deficiency in knowledge and skills in the evaluation of IT solutions negatively affected the efforts of decision-makers who wanted to evaluate the applications.

**ii. Lack of suitable tools for use by small and medium enterprises in evaluating cloud applications**

Furthermore, the findings show a strong perception by decision-makers that there was a lack of tools and methodologies suitable for them to evaluate Cloud BI. There was a strong feeling among decision-makers that the tools and methodologies in use today were difficult because they demanded a high level of technical skills and knowledge. The lack of suitable tools available to SMEs when evaluating BI in the cloud was perceived as a serious challenge that decision-makers faced time and again (mean score 3.1; SD=0.9 by 81.4%, respondents).

Existing literature shows that the lack of standardisation among different CSPs makes it difficult for potential adopters to use a single tool to assess cloud services from different service providers or vendors (KPMG 2016; Sahandi et al. 2012). According to Lewis (2012) standards are essential in cloud computing to enable users to check for compatibility issues among various providers. A

study by Boonsiritomachai et al. (2014) showed that existing tools in BI were suitable for LBEs and SMEs found them difficult to use.

Most decision-makers, 78.9%, indicated that it was very difficult to assess the reliability of user authentication features of Cloud BI applications, one of the areas vital to security. The assessment of authentication features of an application is well-documented (Yauri & Abah 2016) with regards to LBEs who have technical staff but very little information is available regarding SMEs. Although it could be possible for SMEs to evaluate Cloud BI interfaces, the majority, 82.4%, were concerned that without appropriate evaluation tools, it would remain difficult to establish security controls that CSPs claim to provide (mean score 3.0; SD = 1).

Studies show that in the public cloud, CSPs and the client provide security to the data (Perkins 2016; Choi & Lee 2015), but it is difficult for the latter to ascertain that the former has done so (Elena & Johnson 2015b; Romes 2015). The client is always expected to make sure that the right security controls for data in the cloud are in place (Wise 2016; Akinbi 2015). The separation of data in the cloud is a major concern that decision-makers were encouraged to evaluate. Close to 66.6% of the decision-makers stated that the lack of appropriate evaluation tools made it difficult for them to assess the ability of the shared cloud environment to maintain the separation of data belonging to different customers.

The literature emphasises the importance of CSPs to keep secure data separation in the cloud for all clients using cloud services as a cost-effective method for storage, processing and memory functions (Evelson & Bennett 2017; Hazell 2014). By keeping the data separated, each enterprise's cloud service will not be interrupted or compromised by the service or data of another client (Hazell 2014; Kaur & Vashisht 2013). Decision-makers who were suspicious of mixing their data with that of their competitors were met with the challenge to evaluate this aspect without appropriate tools and methodologies for SMEs. Assurance of data separation depends on the type of service an enterprise uses as each service has its risks (Gadia 2018; Hazell 2014). However, the assurance of trusted boundaries is very small in cloud environments compared to on-premise systems (Solanki & Nabeel 2014; Kaur & Vashisht 2013).

Besides the difficulties in evaluating the application, 76.9% of decision-makers perceived the evaluation of the survivability of CSPs as being serious (Mean  $\pm$  SD = 3.0  $\pm$ 0.6). Evelson and Bennett (2017) encourage enterprises to evaluate the viability and survivability of CSPs to avert the risk of vendor lock-in. However, the authors are not precise on how enterprises could do this when they do not have physical access to the CSPs and vendors. According to Greer (2010), SMEs should avoid risky situations by insisting on the assurance of the long-term survival of CSPs. Getting assurance from CSPs proves to be a big challenge for decision-makers due to the lack of historical information about survivability and tools to assess and evaluate this aspect.

### **iii. Challenges of getting relevant information about Cloud BI from the CSPs and vendors**

Regardless of the promises made on the websites of CSPs, decision-makers continue to experience difficulties in getting relevant and useful information needed to evaluate cloud solutions. Decision-makers indicated that the information on the websites and that from friends did not cover all areas they thought could be evaluated, therefore the need to source information directly from CSPs. Most of the information on CSPs' websites was mainly on adverts, incomplete, outdated, unreliable and difficult to understand, making it unsuitable for evaluation purposes. For decision-makers to be able to evaluate Cloud BI, they needed to know how applications functioned and their requirements, historical information about previous security breaches, information on contracts or SLAs, security assurance, reliability, and the physical location of the CSPs. The mean score rating of 3.2 to 3.6 (SD = 0.7) by at least 77.2% of decision-makers confirmed that obtaining various types of information about BI from CSPs was a serious challenge as the providers were not forthcoming. This finding shows that CSPs were unprepared to share information about the safety of the Cloud BI with clients as they claimed on their sites. Without historical information about security breaches and vulnerabilities and the trust and reliability of the Cloud BI, decision-makers perceived the evaluation process as being very difficult to carry out. Lack of co-operation from CSPs made decision-makers suspicious of CSPs concealing security flaws and their deficiencies in providing quality services. Some websites contained outdated information as they had not been updated for years and some email addresses were out of use.

The findings are consistent with other studies in IT solution evaluation that emphasise the importance of gathering information about new technology (Salim et al. 2015; Jabbar, Saleem,

Gebreselassie & Beyene 2003). According to Ettlie (1980), information gathering occurs from the interest stage and continues to the evaluation stage. However, information gathering in previous studies was restricted to friends, experts, salespersons, and websites (Salim et al. 2015, 2016), unlike in this study, where information had to be sourced from CSPs who were remotely situated and inaccessible to decision-makers. This study found that communicating with CSPs regarding their services and solutions, particularly security issues, was a challenge that affected decision-makers' efforts to evaluate the application. Sharma, Apoorva, Madireddy and Jain (2008) highlight the importance of the need for CSPs and clients to have an acceptable level of shared knowledge of the components and services being provided by the former.

A study by Mortimer and Laurie (2019) on the relationship between agency and clients reported a breakdown in trust between the two due to communication problems. The study found that the utilisation of a new channel of communication has shifted the balance of power from agency to client, with the client having the power to reward, punish, or push the agency to comply with contracts (Mortimer & Laurie 2019). In this study, it was not clear whether the CSPs were deliberately ignoring the clients, or if they had closed down. However, the inability of decision-makers to get the information needed for evaluation purposes was a challenge in the evaluation process. With so many CSPs available, some of these could have realised how vulnerable they were from the demands of clients to provide information about Cloud BI as well as their location.

### **The importance of understanding the security evaluation of Cloud BI by decision-makers**

Besides knowing Cloud BI, the study established that decision-makers regarded knowledge and skills in the evaluation of Cloud BI as important for their enterprises to adopt and use cloud technologies. The importance of understanding Cloud BI evaluation was found to be important in three ways, namely, the need for decision-makers to be accountable and responsible for security issues in the enterprise; decisions being based on evidence and security experiences; and knowledge of and skills in software evaluation that improve security assessment and selection of the most appropriate solutions for supporting business objectives in SMEs.

**i. Decision-makers are accountable and responsible for security issues in the enterprise**

The findings from the two surveys corroborate that decision-makers were aware of the importance of participating in the evaluation process because they were responsible and accountable for all decisions affecting business operations and consequences. During the interviews, decision-makers expressed strong feelings that their participation in Cloud BI evaluation could improve their decisions on which technology to adopt and plan for its meaningful use in the enterprise. Decision-makers were convinced that they can only adopt Cloud BI when they were knowledgeable about the security evaluation of the applications. Literature shows that the security culture is the ownership of security principles by individuals in enterprises, particularly owners and managers, who hold themselves accountable for the protection of the information assets they use (Igli & Solange 2019). This was further confirmed by 80.8% of the decision-makers who accepted that they are liable for all security breaches on enterprise data stored in the cloud. These decision-makers affirmed that accountability and responsibility for security issues in the enterprise required a good understanding of security evaluation. Decision-makers could achieve a high level of responsibility and accountability in IS if they become knowledgeable about application evaluation and basic cybersecurity awareness.

According to Weiner (2011) and European Union Agency for Network and Information Security (2015), tactical security risks for businesses using IT solutions were the same, regardless of the enterprise size, and this required security personnel to understand good security practices. In SMEs, there are no security personnel, hence, this crucial task falls in the hands of decision-makers. The findings show that decision-makers acknowledged that they were responsible and accountable for all decisions of different types of ITs to adopt and their use. Therefore, decision-makers needed to complement advice from specialist with their own knowledge and experience in Cloud BI. These findings imply that decision-makers who had knowledge and skills in the evaluation of IT systems were likely to have a better understanding of the security of Cloud BI and improve their accountability and responsibilities. Instead of over-relying on IT specialists, decision-makers were prepared to take a leading role in the evaluation of cloud applications to justify the selection of certain applications.

## **ii. Promoting evidence and experience-based decision-making**

The finding shows the importance of personal experience, knowledge, and skill in the technology adoption process. Decision-makers were convinced that better decisions can be made using existing evidence and their personal experience in evaluating Cloud BI and the cloud environment in general. A mean score of 4.2 (SD = 0.8) by 84.1% of the respondents affirmed that a good understanding of security evaluation was important for decision-making that was based on evidence and experience. This implies that decision-makers who had good knowledge and experience in the use of Cloud BI were able to identify flaws in the applications before investing in them. If decision-makers have experience in evaluation, they will not accept, adopt, or use applications at face value until they have scrutinised them and are convinced of their safety.

The experiences and knowledge in security evaluation acquired by decision-makers could supplement specialist knowledge and advice which is usually scarce, particularly in small towns. The notion of self-reliance was emphasised to expedite adoption when advice from IT specialists was not forthcoming. In the technology adoption process, potential adopters are compelled to acquire new knowledge and experience through hands-on activities and observation of other users of technology, upon which a decision, based on the new experience, is made whether to adopt, reject or defer the adoption and use of the technology (Salim et al. 2014; Chen & Storey 2012; Jabbar et al. 2003). Decision-makers thought that by actively being involved in evaluation activities, they would acquire the knowledge and skills needed. The knowledge and skills were important in preparing decision-makers to cope with challenges brought on by the rapid changes in cloud technologies from various vendors whose safety could not be assured at face value (Cloud Industry Forum 2019; Bills 2012).

Knowledge and skills to do evaluations are vital for decision-makers to be able to use various applications. It will familiarise them with vulnerabilities in technology, cyber threats that are likely to exploit the flaws and assist them to mitigate these threats and vulnerabilities (Zineddine 2015; Khanagha et al. 2013; Sen 2013; Cloud Security Alliance 2011). The hands-on approach to solving IT problems affecting SMEs was important for a lasting solution and to augment other sources of knowledge in security evaluation.

### **iii. Good knowledge and skills in application evaluation improve security assessment in small and medium enterprises**

This finding showed a positive inclination to the importance of understanding Cloud BI evaluation among decision-makers in SMEs to improve knowledge and skills in security assessment and selection of Cloud BI to meet enterprise business needs. The sense of being independent of salespersons and software vendors was an encouragement for decision-makers to seek means to acquire basic knowledge and skills in security evaluation so that the enterprises benefited despite the challenges of lack of support (Angeles 2013). Some decision-makers were convinced that by assessing Cloud BI, they could personally check and verify the suitability of the application against their security expectations and those provided by CSPs.

Most of the decision-makers, 84.2%, with a mean score of 4.2 (SD = 0.8), affirmed the importance of understanding security evaluation as a means to improve security assessment in SMEs. Furthermore, the knowledge of Cloud BI evaluation would enable decision-makers to improve their knowledge in security evaluation so that they could assess the basic security features in the system. Indriasari, Prabowo and Hidayanto (2018) encourage cloud service users to evaluate vendor maturity, as well as matching the features of Cloud BI to those that are most suitable to their business to enable them to further investigate the services offered. Lack of specialisation in SMEs implied that there is no clear difference between work and the personal use of different computing devices and this requires decision-makers to be educated on how to assess and mitigate risks in the enterprises (Weiner 2011). One way to achieve this feat was to encourage decision-makers to actively participate in IT evaluation programmes as much as possible.

### **Effects of lack of understanding of the evaluation process on the adoption and use of cloud business intelligence in small and medium enterprises**

The lack of understanding by SMEs of security evaluation leads to the selection of inappropriate technology solutions and a reluctance to adopt and use Cloud BI in general.

#### **i. Selection of inappropriate technology solutions**

The selection of inappropriate Cloud BI was perceived as a direct consequence of the lack of knowledge of functionalities and security features of existing cloud technology by decision-

makers. Decision-makers felt that they did not have enough functional knowledge of the specific Cloud BI and lacked relevant skills to assess security vulnerabilities and security features in them. A mean score of 4.2 (SD = 0.8) by 86.0% of the decision-makers affirmed that poor understanding of the security evaluation of Cloud BI led to the selection of inappropriate technology solutions. Without the essential knowledge and skills to evaluate Cloud BI, there was a greater chance of selecting inappropriate applications. Decision-makers prefer to avoid making such mistakes by delaying the adoption of new technologies for business use. This finding emphasises the importance of both how-to-knowledge and principle-knowledge (Sahin 2006; Rogers 2005) with which decision-makers should evaluate Cloud BI. For SMEs that fall in the early and late majority, the chances of selecting the wrong Cloud BI solutions increased with the lack of the how-to-knowledge and principles knowledge of evaluation. Chao and Chandra (2012) opine that SME decision-makers find ways to improve their knowledge in various areas of IT use, security assessment and risk management to cope with emerging technologies.

#### **ii. Reluctance in the adoption and use of Cloud BI by SMEs**

Another negative effect of the lack of understanding of evaluation was the reluctance to adopt and use Cloud BI in SMEs. The finding indicates that the willingness to adopt and use Cloud BI was negatively affected by decision-makers' lack of knowledge of the applications to use, how to use them and how the application worked. A mean score of 4.3 (SD = 0.6) by 85.9% of the decision-makers confirmed that poor understanding of the security evaluation of cloud service led to the reluctance in the adoption and use of Cloud BI by SMEs. Insufficient knowledge to evaluate security in Cloud BI was a challenge that led to the delay in the adoption process because decision-makers needed to be confident in the technologies they wanted to adopt. Existing literature confirms that SMEs are reluctant to utilise Cloud BI due to uncertainty in the security of data and applications (Cloud Standards Customer 2017; Ahmed & Hossain 2014; Cloud Security Alliance 2013) which they cannot assess. Govender and Pretorius (2015) argue that without basic skills and knowledge, decision-makers may adopt a wait-and-see stance to assess the success of the new technology to avoid repeating risky decisions which would be costly to the enterprise.



#### **5.2.4. Challenges faced by small and medium enterprise decision-makers when evaluating cloud business intelligence**

The critical challenges preventing SMEs from adopting and using Cloud BI were summarised into five categories. Each of the challenge categories is discussed separately in subsequent subsections.

##### **Uncertainty about information and data security due to vulnerabilities, threats, and cybercriminal activities in the cloud**

This finding illustrates that beliefs and perceptions about security breaches by cybercriminals, such as hackers, were prevalent among decision-makers, and this posed a critical challenge when adopting Cloud BI. Threats to data and information in the cloud environment, particularly those accessed over the web, were regarded as major drawbacks for the decision-makers in recommending the adoption of Cloud BI. Decision-makers were aware that vulnerabilities in cloud technologies could be used by cybercriminals to access their data for malicious purposes (Rayome 2019; Rizvi et al. 2018). This challenge caused decision-makers to be very cautious in their approach to Cloud BI adoption and use.

Decision-makers were worried primarily about the security controls and functionality of unfamiliar applications and the possibility of having malware in their information systems because of adopting Cloud BI with security flaws. The idea of sharing the same data storage with competitors in the cloud was perceived as having the biggest adverse effect on the effort to adopt Cloud BI, particularly in the public cloud (Kersten 2018; Devesh et al. 2017). Decision-makers were afraid of theft, corruption, or deletion of enterprise data and information by hackers or their competitors in the event of data leakages. This concern emanated from the rise in hacking activities that increased the prospects of data, confidentiality, integrity, and privacy breaches in the cloud. A study by Papachrisdoulou et al. (2017) found that SMEs faced challenges, such as data and software errors, such as inadequate security functionality in a cluster of BI tools whose functions were a mismatch with the enterprise's needs and existing ITs. Several studies report that SMEs use functionality and the environment where the applications will be used as the criteria to select BI solutions (Nenzhelele & Pellissier 2014). Literature from cloud security studies (Devesh et al. 2017; Rivastava & Kumar 2015; Sen 2013; Cloud Security White Paper 2011), which highlights

the dangers of adopting cloud services without due diligence, especially the community and public deployed ones where there are high possibilities of clients sharing the same storage and data leakages occurring, supports these findings.

The two cloud deployment models, the public and community, which are accessible and affordable by SMEs, are susceptible to cybersecurity threats that exploit flaws in the technology, resulting in multiple security risks to the enterprises' information assets (European Union Agency for Network and Information Security 2015; Venters & Whitley 2012; Thompson & van der Walt 2010). Some studies report that by adopting Cloud BI, SMEs would be liable to manage threats and risks to their information and data in the cloud (Ashktorab & Taghizadeh 2012; Tiwari & Mishra 2012), a process they could be unable to achieve (Kersten 2018; Bilal et al. 2014). The existence of cloud service models that different CSPs provide makes it difficult to assure and guarantee security to enterprise data in the cloud (Chou 2013; Sen 2013; Tiwari & Mishra 2012; Zunnurhain & Vrbsky 2010). This scenario creates a dilemma for most of the decision-makers who might develop an interest in the adoption but are unable to evaluate the applications by themselves.

Besides vulnerabilities and threat challenges, the findings showed that data and application interoperability and portability were challenges that decision-makers feared would render their data inaccessible and unusable once uploaded to the cloud. The contentious issue raised by decision-makers was whether the applications being offered could open data files without corrupting them (Mirai Security 2019; Chou 2013). Decision-makers were worried about what would happen to their data when enterprises decided to leave one CSP for another. These issues have been discussed in many studies without any solutions (Durg & Podder 2020; Olszak 2014). They expected challenges in system compatibilities that could give rise to data security breaches through multiple conversions.

These fears are discussed in existing studies that focus on technical and non-technical aspects of interoperability and portability deterring enterprises from adopting various cloud services (Lewis 2012; Novakouski & Lewis 2012; Bisong & Rahman 2011). Of particular interest is organisational interoperability, which enables organisations to effectively transfer data and information safely using different information systems across different types of infrastructure and geographic regions

and cultures (Novakouski & Lewis 2012; Robinson et al. 2010; Kubicek & Cimander 2009). Decision-makers were unsure of the compatibility issues between Cloud BI and their on-premise systems and were determined to avoid unsafe operational environments that can render information assets unsafe and expose them to exploitation by CSPs and other cybercriminals. These are issues raised in the DoIT, that whenever users have doubt about the security of technology, they tend to delay the adoption. On data and application portability, data lock-in is reported as the biggest challenge as enterprises are afraid that their data might, at some point, be inseparable from the cloud service (Opara-Martins et al. 2016; Fitzpatrick & Lueck 2010). Several studies encourage decision-makers to be cautious, when selecting BI, of the easiness with which data and application components can be moved and reused elsewhere, regardless of the provider, platform, operating systems (OS), infrastructure, location, storage, format of data, or APIs (Cloud Security Alliance, 2011; Kumar & Padmapriya, 2014; Rivastava & Kumar, 2015).

These findings show that SMEs had limited knowledge of security in the cloud. This implies that protecting data in SMEs is a secondary concern to achieving the primary business goal, contrary to CSPs who are specialised in keeping data secure (Amigorena 2019; Patrick 2015). According to Bisong and Rahman (2011), data and information stored in the cloud are considered to have a higher level of security than that of on-premise storage, which can easily be destroyed by natural disasters. However, Angeles (2013) argues that security in the cloud depends on the CSPs, the type of industry an enterprise is in, and the regulations that govern the type of data to be managed in that cloud. Lack of standardisation in cloud technologies and services offered by different vendors and CSPs make it difficult for SMEs to accept the technology without evaluating it.

The need to safeguard data and maintain business continuity obliged decision-makers to maintain the status quo of using traditional ITs rather than exposing the enterprise to cyber threats in the cloud. With so many Cloud BI on offer today, decision-makers face challenges in ascertaining which applications are secure and suitable for their business needs. Literature shows that cloud services can reduce costs to enterprises while potential security risks are proportional. Therefore, any enterprise which seeks to save costs and increase profitability should seriously assess and evaluate security risks associated with the cloud services involved (Manekar & Pradeepini 2017; Angeles 2013; Bisong & Rahman 2011).

### **Challenges related to the trust of cloud service providers**

This subsection discusses four CSPs factors with a negative impact on the adoption of Cloud BI by SMEs, namely, difficulties in migrating data from one service provider to another; mistrust of CSPs to keep enterprise data safe; mistrust of CSPs to adhere to contracts; and loss of data control to CSPs in clouds.

The presence of many CSPs and cloud services on offer was perceived as a major challenge that militated against the effort by SME decision-makers to select the most appropriate Cloud BI for adoption.

#### **i. Difficulties in data migration among service providers**

Predicaments in migrating data and information from one cloud to another or from one CSP to another was a challenge expected by several participants. The worst-case scenario SMEs expected was vendor lock-in in which the enterprise would be unable to export data and its application whenever there was a need to switch clouds or CSPs (Devesh et al. 2017; Opara-Martins et al. 2016; Agostino et al. 2013). Decision-makers regarded vendor lock-in as a security challenge they would not want to experience. SMEs can be vulnerable and restricted to a single CSP or vendor offering services of poor quality.

The problem with vendor lock-in is that it weakens the rights of the client enterprise's bargaining power, allowing the CSP to conduct unethical business, such as increasing prices or even closing down without due notice (Opara-Martins et al. 2016). Another widely reported data migration problem is the failure of CSPs to provide adequate tools, methods, universally compatible data formats, or interfaces for non-IT clients to easily manage data and ensure service portability (Mirai Security 2019; Cloud Standards Customer Council 2016; Soong & Lam 2015). This makes it difficult for clients without technical skills to switch their enterprises to prospective CSPs with better services or from on-premises to cloud environments (Small Enterprise Development Agency 2020; Opara-Martins et al. 2016; Subashini & Kavitha 2011). SMEs in this study were justifiably cautious to avoid the financial loss of hiring experts to assist with moving their data to new service providers. Therefore, lack of assurance in solving such a challenge by CSPs is a deterrent to the uptake of Cloud BI by SMEs in the selected towns.

In a difficult economic environment, there are chances that a CSP can go bankrupt and close down unexpectedly, locking the application and data for the enterprise in the defunct cloud, a situation that requires due diligence from decision-makers. Vitti et al. (2014) describe this risk as a long-term viability service. Besides shutting down, a CSP can merge with another, resulting in new policies that lead to the loss of data by SMEs (Vitti et al. 2014). The impact of this challenge was rated moderately high, with a mean score of 3.4 (SD = 0.7) by 93.1% of the decision-makers, showing a high awareness of the possibility of some CSPs and vendors going bankrupt and ceasing operations, leaving their clients in the lurch. These findings were supported by Angeles (2013) who observes that enterprises get frustrated when they visit the website of the provider and discover that it is no longer available or inaccessible.

### **iii. Mistrust of Cloud services providers in keeping enterprise data safe**

Mistrust of CSPs led to decision-makers being afraid to subscribe to malicious CSPs, who could, with the help of their employees, gain access to clients' data and compromise integrity and confidentiality, raising the prospects of risks, such as revenue loss and reputation damage. The impact of mistrust of CSPs in keeping enterprise data safe after the adoption of Cloud BI was rated as immense with a mean score of 3.51 (SD = 0.6) by 77.9% of the decision-makers. This finding shows how difficult it was for decision-makers to trust CSPs with their data. The perception of loss of data through theft discouraged decision-makers from adopting Cloud BI.

Literature shows that lack of trust in CSPs is repeated as a major constraint that enterprises experience when they intend to adopt and exploit the benefits of cloud services (Werff et al. 2019; Huang & Nicol 2013). Literature shows that Cloud BI in SaaS pose a security challenge as clients can easily access applications over the Internet via web browsers on various types of network devices (Akinola & Odumosu 2015; Sheshasaayee & Swetha 2015; Hooda 2014). According to ISACA (2011), besides offering clients unlimited computing resources, CSPs provide an easy-access free or low-cost registration process which makes it easy for malicious users to start using the services immediately and anonymously. ISACA (2011) asserts that the free limited trial periods for Cloud BI can be used by hackers to breach the CIA of data and applications residing in the cloud. Worse still, PaaS provides hackers with tools to find the vulnerabilities of the cloud as well

as writing malicious code to disrupt the normal operations of the services (Chang, Kuob, et al. 2015; Chou 2013). This has the potential to expose the cloud services to security threats, vulnerabilities and risks that CSP may not be able to manage (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013). According to Vitti et al. (2014), data recovery is not likely to occur if a CSP fails to assist the enterprise to recover data completely, which can result in non-availability of data and loss of business for the enterprise.

The finding indicates that decision-makers face the challenge of discriminating between genuine service providers and fake ones which may lead to the risk of exposing enterprise data and information to cyber-attacks. For example, Claycomb (2012) posits that due to the availability of several CSPs, it is up to the client enterprise to make an effort to assess each case for potential cyber and inside threats. According to Yu, Li, Hao, Li and Zhao (2017), the lack of transparency in cloud services causes enterprises to mistrust CSPs and the cloud. This complicates cloud security issues and makes it difficult for SMEs to establish whether the CSP would be able to provide sufficient data protection in the cloud (Soofi, Khan & Amin 2014). Some studies show that CSPs rarely provide proper controls to limit access to clients' data by CSPs' employees and this poses a risk to the security and privacy of clients' sensitive data (Hussein & Khalid 2016; Sen 2013).

#### **iv. Mistrust of Cloud service providers in adhering to contracts**

Besides vendor lock-in, the study found that decision-makers doubted the ability of CSPs to abide by their contractual obligations in providing quality services. The mean score of 3.5 (SD = 0.9) shows that the challenge had a big negative impact on the adoption of Cloud BI by SMEs in the Province. Based on their previous experiences with traditional IT, 97% of the decision-makers were sceptical about the capabilities of CSPs in providing services as promised in SLAs and contracts.

The importance of trust of CSPs meeting contractual obligations is stressed in several IS studies. For example, Yu, Li, Hao, Li and Zhao (2017) posit that the reputation of a CSP involves layers of many clients, but that trust is between the CSP and an individual enterprise based on the contracts that exist between the two and the ability of the former to meet the contractual terms.

Several studies encourage clients to trust the CSP only after verifying the facts upon which the trust is built, particular the SLAs (Huang & Nicol 2013). For CSPs to be trusted, they need to be transparent and accountable in service providing (Mesbahi et al. 2018; Huang & Nicol 2013).

Poor-quality cloud services are reported to be very expensive and problematic to correct once the contract is in use (Manekar & Pradeepini 2017; Angeles 2013). The lack of industry standards leads to each CSP having its cloud agreements or SLAs with unnecessary complex jargon designed to confuse potential clients to enter into agreements (Cloud Industry Forum 2019; Ren 2019). Non-adherence to contractual obligation was linked to financial risks whereby the CSP would increase subscriptions or introduce hidden costs that clients should pay to access additional functionalities. According to Hooda (2014), extra costs emanating from the use of Cloud BI prevented SMEs from adopting and using Cloud BI. Decision-makers expressed that they were powerless to compel CSPs to adhere to their contractual obligations if they dishonoured them. CSPs were perceived as being manipulative in the manner they advertised their services and products, designed to lure unsuspecting clients, and make demands later, which frustrated clients (Khorshed et al. 2012). Increasing subscription fees while providing substandard services was a deliberate breach of contract that decision-makers were sensitive to, and they tried to avoid vendor lock-in and financial risks. The dishonouring of contractual obligations was common among bogus CSPs whose websites would merely disappear from the web or were not updated regularly to meet the expectations of their customers.

**v. Loss of data control to Cloud service providers in the cloud**

Most decision-makers believed that by putting data and information on the cloud, they would automatically surrender control to CSPs who could use these for other purposes. This was substantiated by a mean score rating of 3.4 (SD = 0.7) by 64.8% of the decision-makers that possible loss of data control to CSPs prevented clients from uploading to the cloud. There is a plethora of literature regarding the adverse effects of perceived loss of control over data and information as a security challenge, which negatively affect the likelihood of enterprises moving their data and information to the cloud (Papachristodoulou et al. 2017; Hooda 2014). Some studies allude to situations where CSPs could be compelled by law to avail sensitive data and information if demanded by governments of other countries (Senarathna et al. 2016; Vitti et al. 2014; Sen

2013). This is a security challenge that causes decision-makers to suspect that CSPs would expose their data without consent. Cloud clients have reported that they tend to lose data and application control and are forced to depend mainly on SLAs which define the conditions they operate under and are usually biased towards the CSPs (Cloud Standards Customer Council 2016; Hussein & Khalid 2016). This finding confirms that decision-makers did not want to cede the security responsibility of their data to CSPs. However, in public clouds, clients lose both ownership and data control to CSPs, a development that decision-makers are displeased with (Vasista 2015). A study by Mashandudze and Dwolatzky (2015) established that loss of data control to CSPs negatively influenced the adoption of cloud computing technologies among SMEs in South Africa.

### **Financial risks due to data unavailability and corruption in the cloud, stalled operations, or litigation**

Findings show that the financial risks associated with the adoption of Cloud BI harmed the chances of decision-makers recommending the adoption and use of cloud services. Four challenges relating to financial risks were found to have a moderate to big impact (mean scores 3.4 to 3.6) that prevented SMEs from adopting Cloud BI, namely, fear of financial risks due to loss of business, fear of financial risks due to litigation, fear of financial risks due to ransomware, and fear of financial risks due to hidden subscription costs.

#### **i. Fear of financial risks due to loss of business to competitors**

Most decision-makers expressed their fear of losing business to their competitors who might be able to access their data about products and markets, particularly customer information. They believed that their competitors could access the data in the shared clouds, from CSPs and their employees, or hackers. The mean score of 3.6 (SD = 0.7) by 95% of decision-makers shows that this challenge was perceived as having the biggest impact on preventing the SMEs from adopting and using Cloud BI. The fear of financial losses by decision-makers emanated from the possibility of business failure once their competitors knew their markets and products. This implied that decision-makers were not prepared to invest in Cloud BI to avoid financial losses that could lead to business failure.



According to Amigorena (2019), data stored in the cloud can easily be shared among many users and easily integrated with other cloud applications raising the prospects of unauthorised access by malicious users. Amigorena (2019) further asserts that unauthorised access remains difficult to detect even in established LBEs with IT security teams. Besides their competitors, enterprises were reportedly afraid that former employees could access the data stored in the cloud from anywhere (Claycomb 2012; Subashini & Kavitha 2011). Studies show that client enterprises fear the possible security breach of customer data stored in the cloud, which can result in financial loss through legal liabilities (Patrick 2015; Subashini & Kavitha 2011). The main objective behind SMEs is profit-making, using minimum investments, which they need to protect. One way of achieving that is avoiding any situation which would put them in a compromised position due to exposure to their competitors.

#### **ii. Fear of financial risks due to litigation**

The finding shows that decision-makers were aware of the financial implications of data breaches emanating from their enterprises. Decision-makers were not prepared to pay any legal costs related to customer data exposure, particularly those in financial services. This was the second challenge that had a considerable impact. A mean score of 3.5 (SD = 0.8), by close to 93% of respondents, affirms that their efforts to adopt and use Cloud BI was affected by the fear of the costs of a lawsuit in the event of a breach to clients' sensitive information. Some SMEs in finance, car sales and accommodation indicated that they would not put their sensitive data in the cloud if they adopted Cloud BI to protect themselves from unnecessary lawsuits. This finding shows that decision-makers who used cloud services had indicated that security risks were not only confined to data breaches but extended to lawsuits that clients could file against the SMEs. Enterprises would want to avoid legal liability by all means (Graham 2017; Angeles 2013). According to Kodagali (2019) enterprises need to evaluate CSPs' legal terms, such as intellectual property ownership, account termination, data retention, and data sharing policy.

#### **iii. Fear of financial risks due to ransomware**

In the interviews, decision-makers did not directly mention ransomware but referred to paying hackers to release locked data and applications. However, perceptions of ransomware were solicited in the QUAN phase to supplement financial risks. Although decision-makers had limited

knowledge about ransomware, the fear of losing finances due to payments towards ransomware was rated to have a significant impact, mean score of 3.5 (SD = 0.9) by 64.9% of the decision-makers.

This finding indicates that decision-makers were aware of hacking activities perpetrated to force enterprises to pay a fee towards the access of their information assets or stop hackers from disclosing sensitive information. According to reports, ransomware has been on the rise (Graham 2017) with approximately 284489 unique users being affected in South Africa alone (Hasbini 2019). A memorable case involved the hacking of the Johannesburg City Power utility web application, which paralysed many service delivery systems (Hasbini 2019). The publicity of such data breaches in the cloud environment reinforces the perceptions among the decision-makers that adopting cloud services such as Cloud BI is a bad idea for SMEs. It has been observed that although the negative impact of data security breaches in many organisations is publicised, the solutions to these challenges are never made public to assist other businesses facing the same problem. Decision-makers with little technical know-how to deal with ransomware would rather opt to maintain on-premise IT systems, which are vulnerable. This finding shows that decision-makers are pragmatic as they always choose a solution which reduces financial risks if their businesses were to remain operationally viable.

#### **iv. Fear of financial risks due to hidden subscription fees**

The study found that SME decision-makers were not prepared to pay hidden costs arising from additional subscription fees. Decision-makers expressed their weariness of bogus CSPs who would charge them higher subscription fees for non-existing services. This challenge had a moderate impact on the adoption of Cloud BI by SMEs, with a mean score of 3.4 (SD = 0.9) by 50.9% of decision-makers. Decision-makers were cautious of SLAs that would lead to additional costs to SMEs who already had constrained budgets. A good case involved bandwidth costs which the SMEs were to settle with internet service providers in addition to CSPs charges (Mashandudze & Dwolatzky 2015). Similarly, Sheshasaayee and Swetha (2015) posit that the main challenges of cloud software are the additional costs that might arise from their use, the limited checking of unused services and their non-establishment within the general public. This finding indicates that decision-makers were unfamiliar with the elasticity and on-demand services which could be

switched on and off and then paid for extra usage. However, Mashandudze and Dwolatzky (2015) apportion the problem to the uncontrollable costs of cloud services compared to on-premise IT solutions which SMEs were familiar with.

### **Limited knowledge of the types of Cloud business intelligence solutions**

Although most decision-makers expressed awareness of Cloud BI and its benefits in data management and decision-making, the study found that they lacked knowledge of the different Cloud BI solutions and how to use the technology. The lack of functional knowledge of specific Cloud BI was perceived as a challenge with a considerable negative impact on SMEs' efforts to adopt the technology. The decision-makers' expression of their inability to use Cloud BI was enough evidence that the knowledge of and the how-to-knowledge were important for the adoption of the technology in the first place.

The importance of knowledge of Cloud BI and the how-to-knowledge required for the decision-making process of adopting technology is emphasised in the studies by Ettlé and Penner-Hahn (1994), Rogers (2005) and Wanjiku and Moturi (2016). In this study, 64,9% of the decision-makers indicated that the lack of knowledge about CSPs' reliability and the lack of knowledge about security vulnerabilities in Cloud BI were perceived as having adverse effects on the adoption of Cloud BI by SMEs in the province.

There was a strong feeling among decision-makers, at least 51%, that a lack of knowledge about security in different cloud deployment and GUI features of Cloud BI was a challenge with a considerable negative impact. All the five challenges related to lack of knowledge about the technology were regarded as strong deterrents to the effort by decision-makers to recommend the adoption of Cloud BI. The findings were consistent with previous studies on the adoption of technology which emphasised the need for SMEs to have sufficient knowledge about the technology they wanted to adopt including safety in the environment (Papachristodoulou et al. 2017; Wanjiku & Moturi 2016; Sahin 2006; Ettlé & Penner-Hahn 1994).

Without the proper knowledge about the CSP reliability and security vulnerabilities, threats, and risks in the cloud, it could be futile for SMEs to adopt Cloud BI as they could face service

disruption, fail to recover their data, and possibly suffer from vendor and data lock-ins (Cloud Industry Forum 2019; Ahmed & Hossain 2014). CSP reliability comprises service availability to customers, the impact of any failure on customers, service performance and business continuity (Cloud Industry Forum 2019; Angeles 2013; Bills 2012; Sahandi et al. 2012) which decision-makers have to evaluate before adopting Cloud BI. However, to accomplish this, decision-makers require knowledge about the Cloud BI and the deployment environment, how the cloud works, and have skills and knowledge to evaluate the technology.

The mean score of 3.5 (SD = 0.7) indicates a high perception by at least 51% of decision-makers that lack knowledge on how the cloud works, lack of skills to identify and select the most appropriate Cloud BI, and an inability to use Cloud BI for business purposes were challenging to the adoption of Cloud BI in the province. This lack of knowledge was compounded by a lack of support from CSPs, which increased frustrations among clients who faced problems during the process of adopting cloud technologies (Papachristodoulou et al. 2017; Angeles 2013). For SMEs to fully utilise and benefit from Cloud BI with baseline knowledge, they would require a lot of support, which is difficult to get from CSPs and scarce IT specialists. Without good functional knowledge and how-to-knowledge of Cloud BI, all the efforts to adopt the technology would be in vain. Govender and Pretorius (2015) purport that knowledge about the environment, the need to be addressed by the technology, and the skills needed to make use of the technology were important for decision-makers to justify the adoption of new technologies. Jabbar, Saleem, Gebreselassie and Beyene (2003) purport that for the decision-makers to adopt, reject or defer decisions depends on the belief derived from the perceptions and knowledge about the benefits and risks the technology can have on the existing operations.

Decision-makers at the evaluation stage regarded Cloud BI as complex to learn how to use, contrary to suggestions by various sources on the open web that claim that cloud services were easy to use by non-technical personnel (Majhi & Dhal 2016). This made decision-makers doubt their ability to use Cloud BI for productive purposes and was complicated by their inability to select the most appropriate applications. Studies show that some enterprises adopt technologies without enough skills to use them (Taherdoost 2018; Patrick 2015; Angeles 2013; Rogers 2005). With many Cloud BI on offer, decision-makers found it difficult to have in-depth knowledge and

skills in one or two such technologies. The challenges posed by the lack of technical know-how to use new technology are reported to be more concerned with prevention factors than the benefits offered by the same technology (Fry et al. 2018; Taherdoost 2018; Meijer et al. 2015; Renny et al. 2013).

### **Physical security issues with CSPs in different jurisdictions**

Some decision-makers indicated a very strong interest to have physical access to potential CSPs before they adopted the technology. This finding was linked to the security of data at various data centres, a concern that made decision-makers think of inspecting these facilities to make sure that they were dealing with existing CSPs. This shows a traditional view of the security of on-premise data centres that existed among decision-makers. The importance of physical security is that it provides enough protection to IT equipment at the data centres to ensure reliability and at the same time, prevent physical intrusion by malicious users (Dhar 2014; Harfoushi et al. 2014). Literature shows that the physical protection of IT equipment at the data centres is essential for the protection of data and information assets (Amigorena 2019), which decision-makers in this study wanted to achieve by conducting a physical inspection of data centres. Decision-makers believed that one of the most appropriate ways of knowing the CSPs was to have a physical inspection of their infrastructure.

This finding further confirms how important physical security at CSP data centres was among decision-makers who were considering adopting Cloud BI deployed in public clouds. Studies confirm that enterprises opting for public and community clouds rely entirely on CSPs for the security of data centres to prevent unauthorised on-site access and theft of data (Chou, 2013; Cloud Security Alliance, 2016). On the other hand, the findings show that decision-makers were not aware that CSPs kept data backups in different data centres, making it difficult for them to inspect these facilities. According to Moore (2014), differences in geographical locations of CSPs and enterprises prevent clients from assessing the physical security in data centres as well as checking the unauthorised access to data by the CSPs and their employees. Although CSPs are required to be transparent about their data centre locations, individual enterprises are expected to assume responsibility for locating the needed information during the evaluation stage (Cloud Industry Forum 2019; Salim et al. 2015).

### **5.2.5. The main components of a security evaluation framework for Cloud BI for small and medium enterprises**

Four findings were made for this SRQ from both the QUAL and QUAN phases. The discussions for each finding are presented under respective subheadings.

#### **Lack of knowledge of tools and methodologies used for evaluating cloud business intelligence**

Although decision-makers were not able to conduct systematic evaluations of Cloud BI, they were familiar with tools, such as checklists, guidelines, procedures, and malware scanners but had little knowledge of models and frameworks for evaluating cloud technologies. This was supported by QUAN findings in which 42.1% of decision-makers confirmed that they were familiar with checklists and 29.8% have used guidelines once in assessing IT applications. The least known tools were models and frameworks as indicated by close to 60% of the decision-makers who never used these tools before.

This finding shows that SMEs do not use standard tools to evaluate IT solutions before adopting Cloud BI, but they depend heavily on what salespersons, vendors within their localities, and even their friends or competitors offer. This is consistent with the Cloud Standards Customer Council (2017) observation that most enterprises adopt cloud technologies and services without proper evaluation due to the limited knowledge of existing security evaluating tools and methodologies. The blame for the challenge is placed on SME decision-makers who view security as a problem for IT professionals rather than a business one (Moraetes 2018; Wild 2018). For managers to understand security frameworks, they have to actively participate in security issues in the enterprise, including the evaluation (Heiser 2019). Literature indicates the existence of many security frameworks used for risk management by enterprises already using IT solutions (Chang, Walters & Wills 2015; Granneman 2014; Greis 2014). Commonly cited security frameworks include a range of common security frameworks (CSF), including the National Institute of Standards and Technology (NIST ISO 27001 series), NIST Cybersecurity Framework SP 800-53, Payment Card Industry Data Security Standard (PCI DSS), Health Information Trust Alliance (HITRUST), CSF and COBIT and ISACA (Moraetes 2018; ISACA 2011). These standard

frameworks have been developed to assist businesses enterprises to protect their IT systems against vulnerabilities, cyber threats, and risks (Mogull et al. 2017; Rivastava & Kumar 2015; Subashini & Kavitha 2011). Lack of knowledge of frameworks and models by decision-makers confirmed challenges to the evaluation of Cloud BI that needed to be solved to assist SMEs in selecting appropriate applications.

### **Knowledge about basic components of a framework that meet the business needs of small business enterprises**

The study found that decision-makers did not have enough knowledge about components of a security framework but mere expectations, such as simple guidelines, checklists, policies, and possible procedures. During the interviews, decision-makers were not confident to answer this question, indicating their lack of knowledge about frameworks for evaluating IT solutions in general and Cloud BI specifically. The finding showed that most decision-makers, 80.2%, confirmed that they expected a security framework for evaluating Cloud BI to comprise instructions, checklists, guidelines. Very few decision-makers, 16%, perceived procedures and models as being components of frameworks. Although decision-makers lacked in-depth knowledge about security frameworks, they suggested that a security framework should have components that provide means by which one could evaluate several aspects of the cloud.

Few studies on the adoption of cloud services have attempted to measure knowledge or awareness of technology among SME decision-makers but overlooked critical issues about the tools used to evaluate the technology to be adopted (Hashim & Hassan 2015; Chao & Chandra 2012). A study by Salim et al. (2015) examined how SMEs moved from evaluation to trial of cloud ERPs and explored the importance of the evaluation process but did not elucidate on whether decision-makers were familiar with the tools they used for evaluating the IT solutions. A study by Kikawa (2019) on the acceptance of BI in the City of Tshwane found that poor knowledge and limited technical skills due to lack of training contributed to the subdued use of the technology by SMEs. However, the study does not discriminate between the knowledge needed to use the technology and evaluation knowledge. The literature about decision-makers' knowledge about evaluation tools remains scarce, regardless of the encouragement that enterprises evaluate cloud services (Chao & Chandra 2012; Olszak & Ziembra 2012). According to Geer and Sullivan (2019), a

framework is loose and flexible enough to allow the addition or removal of elements when necessary to satisfy an enterprise or users. Without the proper knowledge of evaluation tools, decision-makers would continue to use trial and error techniques when evaluating cloud services which eventually leads to the adoption of wrong solutions.

### **Knowledge of decision-makers about the uses of the framework in evaluating Cloud BI**

Unlike previous studies which depended on IT experts and specialists in designing models and methodologies for use by enterprises (Anderson 2017; Constantinides et al. 2012; Winkler 2011), this study was designed to include knowledge from decision-makers to develop the framework for SMEs to evaluate Cloud BI. Due to this, the need to understand decision-makers' perceptions about the use of a framework to evaluate Cloud BI was important. The findings were that decision-makers perceived the uses of the Cloud BI security evaluating framework. The three findings were: checking data security, functionalities of the application, vulnerabilities, and threats in the Cloud BI; making the selection easy and give direction on the safe use of Cloud BI, and guiding users to check how secure software is before its adoption and use.

#### **i. Checking data security, functionalities of the application, vulnerabilities, and threats in the Cloud BI**

The feeling among decision-makers was that a tool, such as a framework was important in aiding the assessment of key areas of the cloud application, including the security of data in the cloud, existing vulnerabilities, risks, and security functionalities in cloud business solutions. Although decision-makers have not used frameworks and models to evaluate IT solutions, they were convinced that these tools would be useful if used appropriately. Most of the decision-makers, 80%, considered a framework to be the most appropriate tool needed to explain to all parties how information systems and services were managed within the enterprise (mean score 2.9; SD = 0.3). Seventy-three percent (73%) of decision-makers (mean 2.8; SD = 0.7) observed that a security framework was helpful to guide an enterprise to identify vulnerabilities and threats in Cloud BI and reduce the risk levels and the exposure of an enterprise's IT information system to threats on the web. These findings show that decision-makers focused primarily on the technical aspects of using the framework in the process of security evaluation rather than the governance of ITs. This indicates the overall bias of decision-makers towards the use of frameworks in the evaluation rather



than the details of using the tool. Literature regarding the use of frameworks by managers to evaluate Cloud BI is scarce. Much of the literature is on security frameworks used for risk management by enterprises already using Cloud BI and other cloud services (Anderson 2017; ENISA 2015; Constantinides et al. 2012; Winkler 2011). The little available literature is important in this study when blended with experiences from decision-makers on the evaluation of Cloud BI.

**ii. Making the selection of Cloud BI easy and giving direction on the safe use of applications**

The finding shows that decision-makers expected the framework to make the evaluation process and choice of Cloud BI very easy as they would find instructions to do so. Decision-makers believed that the framework would assist them to reduce the risks of adopting the wrong technologies and then guide them to use the application safely to improve decision-making in their enterprises. Findings reveal that close to 75% of decision-makers were expecting the security framework to assist them to solve problems when evaluating the suitability of Cloud BI, the cloud environment, and the CSP's reliability to provide services (mean score 2.7 SD = 0.6). They further indicated that without the framework, it would be difficult for decision-makers to conduct an evaluation. Nearly 68.4% of the decision-makers were convinced that a security framework would instil confidence among SMEs in systematically assessing Cloud BI and stop over-relying on friends and IT specialists who charged them for services provided (Mean score 2.6; SD = 0.8). Heiser (2019) posits that some Gartner clients struggle to evaluate the security of several CSPs due to a lack of commonly agreed methods and standards to measure the security maturity of each CSP. Therefore, enterprises unknowingly use unsecured cloud applications and services.

**iii. Verifying whether cloud applications meet the security and operational requirements of the enterprise**

Security and operational requirements of cloud solutions were among the important features that decision-makers perceived should be verified before the adoption of the technology. The framework would make it easier for decision-makers to verify whether the security features of the Cloud BI were commensurate with the enterprise's expectations. Based on the mean score of 2.5 (SD = 0.8), the perception that the framework would assist decision-makers to verify if Cloud BI met security and operational requirements was another major use of the framework confirmed by

70.2% of decision-makers. Decision-makers were confident that the security framework would provide an alternative solution for systematic evaluation of security vulnerabilities, threats, and risks in Cloud BI before the adoption. These findings show that decision-makers needed a framework to assist them to check whether the Cloud BI solutions they were interested in met security standards and operational requirements. Decision-makers were aware of the consequences of adopting unsecured applications which would not meet their operational requirements.

### **Types of frameworks expected by decision-makers**

The findings show that decision-makers did not have any clear ideas of any framework of interest. However, based on their limited knowledge about frameworks, decision-makers elaborated on a security framework they thought would be suitable for them. The expectations of decision-makers on the proposed framework are discussed in this subsection.

#### **i. Simple guidelines on security evaluation of cloud business intelligence**

From the attestations made, it was clear that there was a consensus from the decision-makers that an evaluation tool was needed by SMEs who were at the evaluation stage of Cloud BI adoption. Decision-makers suggested a framework with simple guidelines, checklists, or instructions within the understanding of people with little technical knowledge and skills in IT and security evaluation. This implies that participants need a simple framework within their limited knowledge and skills to assist them with guidelines on how to evaluate Cloud BI. The framework would consider key areas that the decision-makers expected to examine and those suggested by experts.

Wild (2018) found that directors and senior managers in different business setups in New Zealand understood the need for a security framework but were unsure how to proceed. According to Wild (2018), the existence of several similar frameworks would require managers to make a meaningful choice to tailor-make one or more to suit the enterprise's needs. Similarly, Moraetes (2018) posits that several existing security frameworks have redundant features that facilitate IT, security teams, to manage controls to meet compliance with a set of regulatory standards. A good recommendation is to select the controls that best assist an enterprise to meet its business objectives from ISO 27001, National Institute for Standards and Technology (NIST 800-53), and Control Objectives for Information and Related Technologies (COBIT) and develop a hybrid framework (National

Institute of Standards and Technology 2020; Moraetes 2018; Cloud Standards Customer Council 2016; Perkins 2016). Literature shows that there was no singular security framework that satisfied the needs of enterprises of various sizes. Therefore, it was essential for managers to conduct research on the existing security frameworks and make effort to assess the merits and demerits of each approach (Moraetes 2018; Choi & Lee 2015; Ibrahim & Musah 2015; Vohradsky 2012). However, enterprises tend to complain about the time to find information about frameworks.

**ii. An economical and reliable framework to assess cloud business intelligence**

Decision-makers were interested in an economical and reliable security framework that could be used at any stage of the evaluation process. This finding indicates that decision-makers based their judgements on the cost of using a security framework and the reliability of the results it produced. As already alluded to in the previous section, a simple and easy-to-use framework would require decision-makers to invest less effort and money in learning how to use the tool. Decision-makers believed that a framework with simple guidelines would aid them to select the most appropriate Cloud BI without compromising their standing and financial position. The framework was supposed to be generic and used by SMEs in different economic sectors. Due to their financial constraints, SMEs preferred a cost-effective framework that required less time to complete the evaluations. A framework that demanded a lot of time and skill from the users was inappropriate for decision-makers who did not have the required skills and knowledge in Cloud BI solutions. The respondents maintained that the framework should be used to protect SMEs from CSPs by identifying the required standards to evaluate Cloud BI. An economical and reliable security framework was envisaged to reduce financial and technological constraints and risks that SMEs were more likely to face in their quest to evaluate Cloud BI.

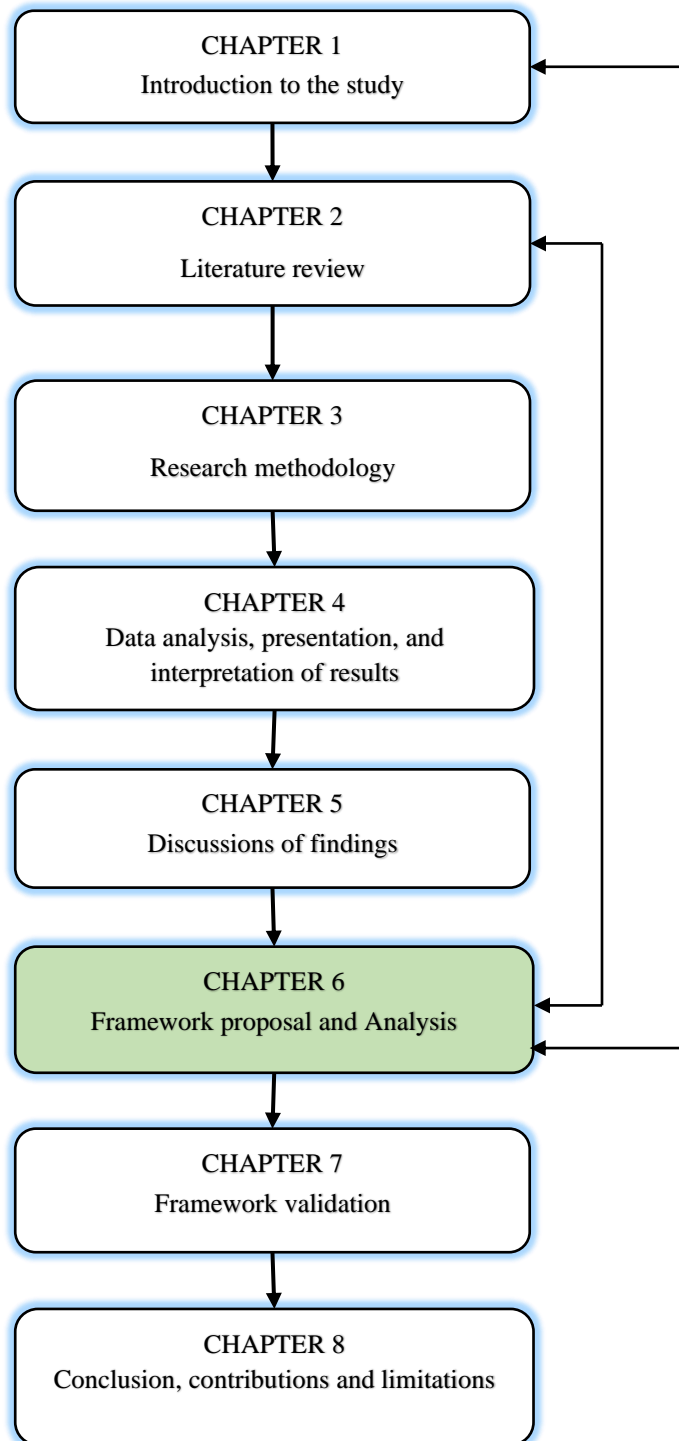
**5.3. Conclusion**

This chapter discussed the findings of the study. Decision-makers of SMEs in Limpopo Province face many challenges when adopting and using Cloud BI. The state of Cloud BI adoption and use in the selected towns was very low, regardless of the high level of awareness of the benefits of Cloud BI among decision-makers. The main challenges were lack of knowledge among decision-makers about Cloud BI and how to operate them, lack of understanding and skills in selecting the appropriate applications, fear of financial risks arising from cyber threats, and mistrust of CSPs.

Decision-makers were concerned that there were no appropriate Cloud BI evaluation tools for use by SMEs. The awareness about Cloud BI among decision-makers was generally good but was not good enough to evaluate these applications. Decision-makers were aware of the potential dangers of adopting Cloud BI without proper security evaluation of threats and risks in the cloud but lacked the strategies, knowledge, and tools to do so. Furthermore, decision-makers recommended a simple and user-friendly security evaluation framework that provided guidelines and checklists to guide the evaluation process.

The next chapter provides insights into the proposed security evaluation framework and the checklists to guide the users when evaluating Cloud BI.

## CHAPTER 6      FRAMEWORK PROPOSAL



## **6.1. Introduction**

The purpose of this study was to propose a user-friendly security evaluation framework for Cloud BI for use by SMEs from five selected towns of the Limpopo Province. The proposed framework is based on the findings discussed in the previous chapter.

## **6.2. Security evaluation framework proposal and analysis**

Chapter 1 of this study has shown that there was no security evaluation framework tailored for the adoption and use of Cloud BI by SMEs in South African small towns where IT specialists were scarce. The existing security frameworks and standards focus much on cloud computing per se, leaving SMEs who intend to adopt Cloud BI with a limited choice of evaluation tools. In Chapter 2, it was indicated that eSentire Managed Security Services (2012) developed a comprehensive checklist to evaluate CSPs; Khan and Al-Yasiri (2015) proposed a road map framework for cloud adoption by SMEs; Cloud Standards Customer Council (2017) provides guidelines for adoption of cloud technologies; the Information Security Forum (2016) developed the Standard of Good Practice for Information Security 2016 for best practice. These initiatives were done mainly in developed countries where SMEs have very good knowledge of cloud security and have stronger support from IT specialists and respective governments. The tools are too complicated for SME decision-makers in remote South African towns due to limited knowledge and the unavailability of IT-specialist to assist the enterprises. Therefore, the solution to the security evaluation problems faced by local SMEs requires a home-grown solution based on these enterprises' best practices in IT, fused with essential aspects of traditional security frameworks and standards. These findings justified the proposal of a security evaluation framework for Cloud BI for SMEs.

### **6.2.1. Factors motivating the proposal and development of the new framework**

The findings of the study showed that the effort and willingness of decision-makers to adopt and use Cloud BI were negatively affected by several factors. The militating factors to the adoption of Cloud BI by SMEs were as follows:

- i. fear of data security breaches and risks due to the exploitation of cloud technology security vulnerabilities by cyber threats;
- ii. limited knowledge about the nature of security provided by Cloud BI and how they worked;

- iii. limited knowledge and skills by decision-makers in evaluating security in Cloud BI;
- iv. lack of knowledge in the use of existing evaluation tools and methodologies because of their complexities;
- v. mistrust of CSPs and their employees in keeping enterprise data safe;
- vi. mistrust of CSPs in meeting their contractual obligations of providing reliable and secure services;
- vii. fear of financial losses due to poor business performance and litigation arising from security breaches of customer data and data lock-in; and
- viii. lack of easy-to-use evaluation tools for SMEs for decision-makers who were actively involved in the selection of IT systems.

The solution to the impending challenges faced by SMEs in the adoption of Cloud BI was to propose a step-wise security evaluation framework, taking into consideration the reality of decision-makers' expectations, experiences, IT knowledge, the technologies they have, and IT evaluation skills. To propose the framework, important aspects arising from the findings were summarised and presented in Figure 6.1, namely, the enterprise data, technologies, services and their delivery, deployment models, people, or enterprise (CSPs, users & clients) and financial benefits and risks. These formed the key aspects to be evaluated before the adoption of Cloud BI by SMEs in the selected towns in Limpopo Province.

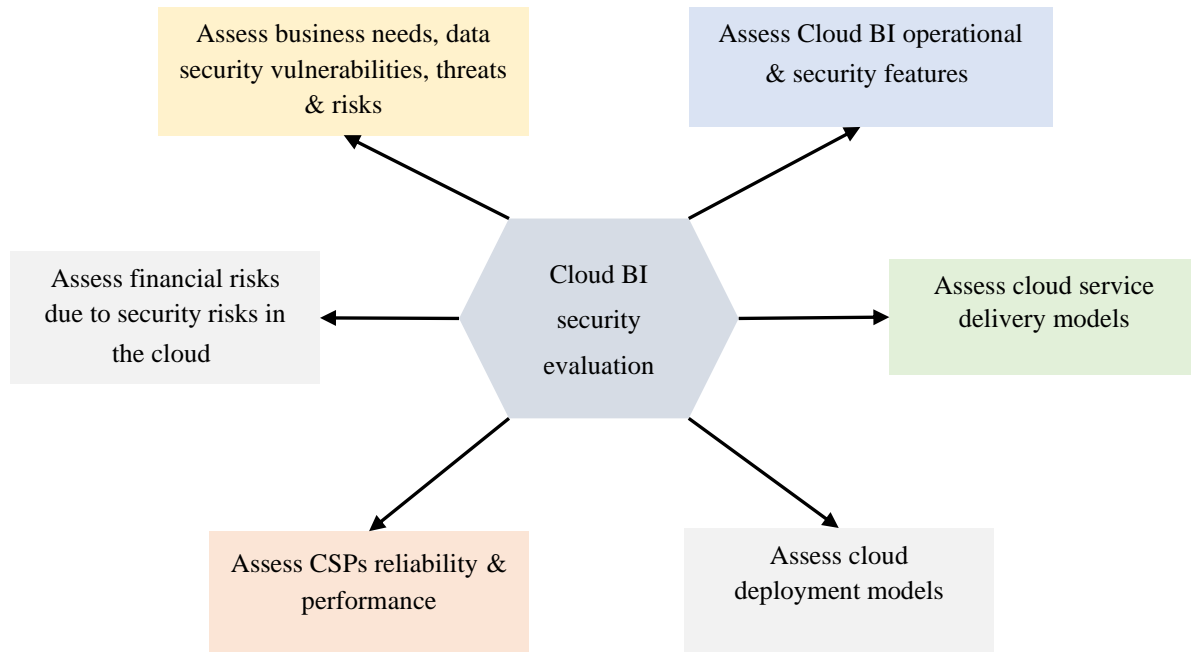


**Figure 6.1: Findings that form the basis of the framework**

Although the level of adoption and use of Cloud BI for business purposes was low, the use of cloud services on a personal level was appreciably higher, judging from the good security awareness among decision-makers and the considerations they suggested for the evaluation process. Decision-makers' willingness to evaluate Cloud BI to aid in the selection process hinged on the availability of appropriate and easy-to-use evaluation tools and techniques. This suggests that decision-makers expected the proposed framework to be simple, economical, safe, and reliable for use by a non-IT specialist. The conceptualisation of the framework considered the critical challenges faced by SMEs when adopting Cloud BI, several activities that decision-makers regarded as important when evaluating Cloud BI. Figure 6.1 shows the areas to be evaluated, which were derived from the findings of this study. Six major components of the framework were



considered for a comprehensive evaluation process of Cloud BI, namely: 1) business and data security needs; 2) Cloud BI operational and security features; 3) security of cloud service delivery model; 4) security of cloud deployment models; 5) cloud service providers; and, 6) financial risks to the business enterprises emanating from using Cloud BI. Figure 6.2 shows the six components of the framework that should be considered during evaluation.

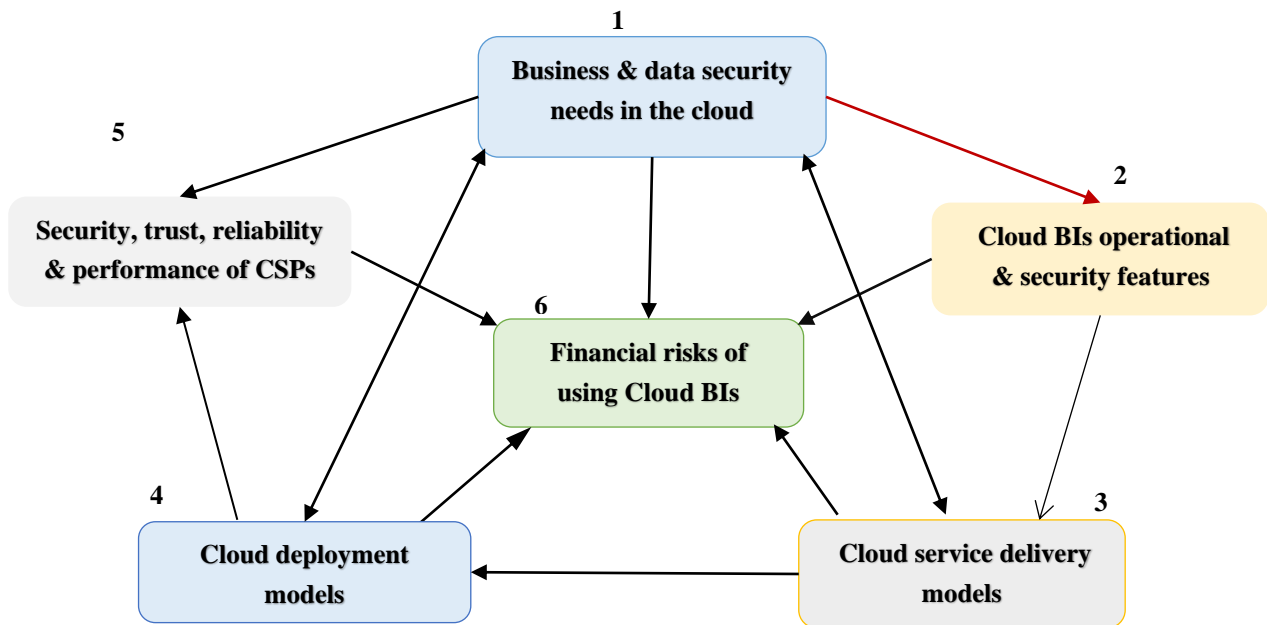


**Figure 6.2: Components of security evaluating framework for Cloud BI**

### 6.2.2. The Cloud Business Intelligence Security Evaluation Framework

The Cloud Business Intelligence Security Evaluation Framework (CBISEF) provides a structure intended to support the evaluation and selection processes, and efforts of decision-makers in various SMEs without relying on IT specialists. The CBISEF addressed six major areas where SMEs faced challenges when adopting Cloud BI. The CBISEF was meant to be flexible so that SMEs could customise it by adding or removing components to meet their needs and expectations. Figure 6.3 shows the interrelationship of the six components of the proposed CBISEF with the focus on financial risks, which SMEs prioritise in the evaluation process. Data security and financial risks are emphasised in the other four components of the evaluation process and provide the fulcrum of the framework. The CBISEF focuses on issues within the reach of non-IT specialists

who are proficient IT end-users with basic knowledge of information security, particularly Cloud BI and cloud services.

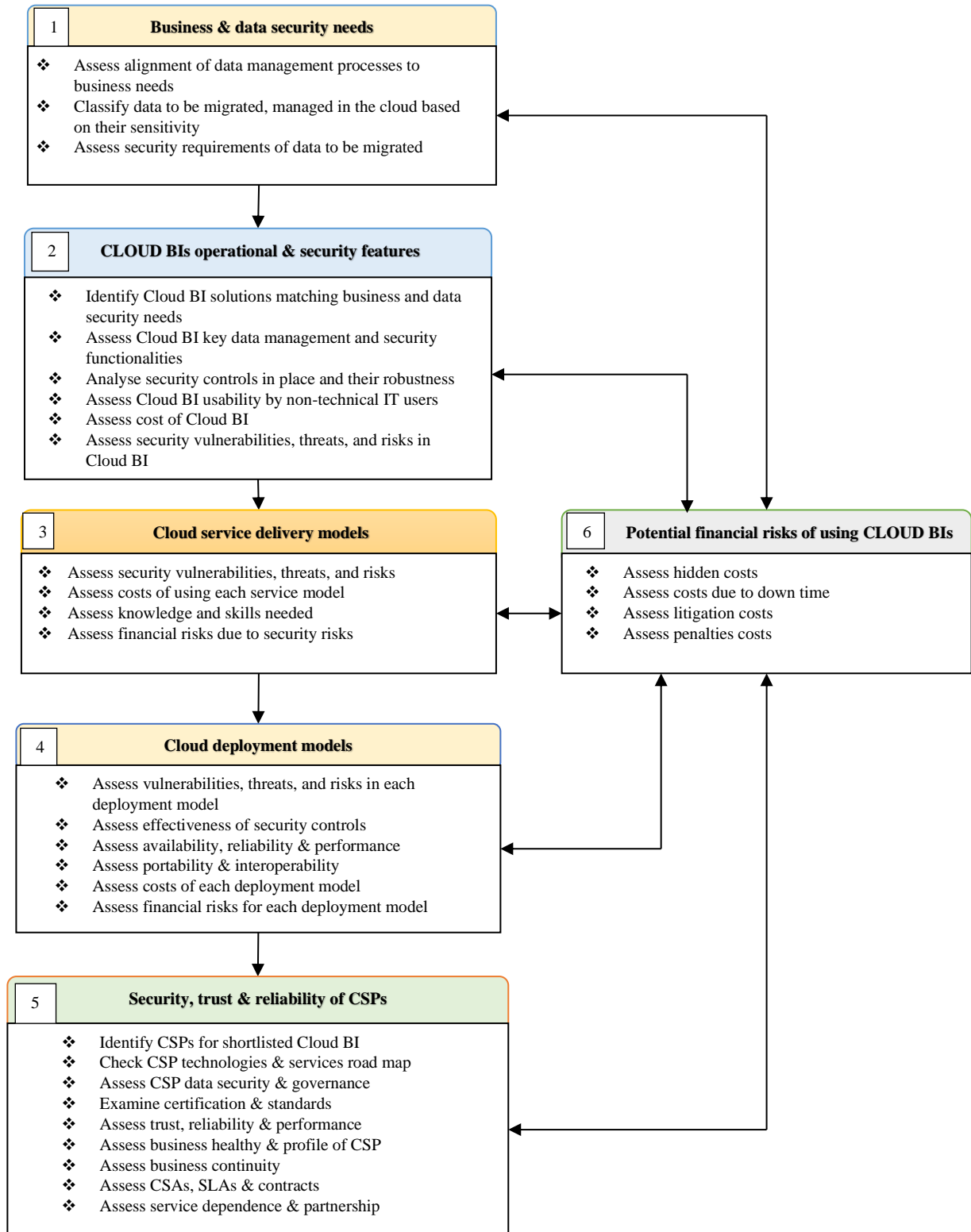


**Figure 6.3: Cloud Business Intelligence Security Evaluation Framework for SMEs**

The purpose of the CBISEF was to assist SME decision-makers with the aspects to evaluate before the adoption of the Cloud BI. The proposed framework was intended to be a stepwise guide that decision-makers could follow when evaluating Cloud BI. Each component consisted of activities that needed to be examined during the evaluation process. Each component of the CBISEF is elaborated in the framework analysis section. A checklist for each component was designed to guide users of the framework during the evaluation process. Figure 6.4 is the expanded diagram of the CBISEF.

### 6.2.3. Framework analysis

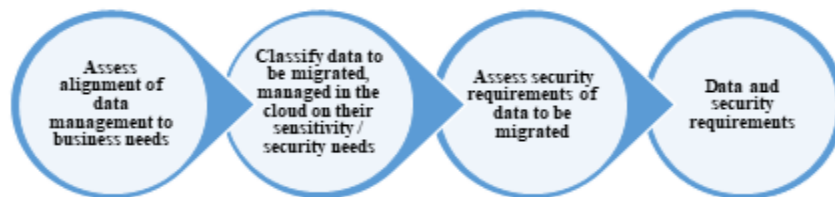
A detailed description of the CBISEF is given, based on each of the six components, and diagrams elucidate the important activities that the evaluator would perform. A checklist is provided with a set of criteria for the evaluation of each component. The expanded diagram for the CBISEF in Figure 6.4 shows details of the activities to be done during the evaluation process.



**Figure 6.4: An expanded security evaluation framework for Cloud-BI**

## Assessment of business and data security requirements in the cloud

The first stage of the security evaluation process is intended to assess the preparedness of an enterprise to adopt and use Cloud BI or any other cloud service. Several studies highlight that data and information are the most vital enterprise assets required for decision-making and the need to prioritise its security (Jakimoski 2016; Lacity & Reynolds 2014; Juan-Verdejo & Baars 2013). The proposed CBISEF took into account data security and protection in line with the business needs of an enterprise (Fernandes et al. 2013; Shimamoto 2015). To this end, the CBISEF required decision-makers to assess business needs and security requirements for data that should be migrated to the cloud and managed by Cloud BI. Drye and Warren (2015) argue that enterprises should evaluate their business needs, data requirements, and risk at the onset of the evaluation process. Figure 6.5 shows key activities which can be performed at the beginning of the evaluation process of Cloud BI.



**Figure 6.5: Business needs and security requirements for data to be migrated to the cloud**

### *i. Assess alignment of data management plans with business needs*

In the CBISEF the evaluation process should begin with decision-makers assessing the alignment of enterprise data management plans with key business needs. According to Gralewski (2017), data management plans refer to strategies used by an enterprise to store, migrate, protect and process data. Previous studies report that decision-makers who are not aware of the importance of data and information in decision-making in future business operations hardly had any meaningful data management strategies for their information systems (Richardson 2017; Lacey & James 2010). Decision-makers first need to understand their data sources, collection methods, processing, and use and then identify weaknesses that require remedies to improve the quality of information for decision-making (Gralewski 2017; Richardson 2017; Bilal et al. 2014). Decision-makers identify different types of data according to processing schemes (manually or electronically) and identify the business objectives supported by each data set. Decision-makers would then be able to set clear rules on how data will be managed to support the business objectives using Cloud BI.

While accomplishing this activity, decision-makers are expected to account for existing business and technology commitments needed for their enterprises to address business objectives.

**ii. Classification of data to be migrated, stored, and managed in the cloud, based on the sensitivity or security needs**

In this activity, decision-makers identify all data that need to be migrated, stored, and managed in the cloud and then classify it according to the security requirements needed to keep it safe in the cloud (Kelley & Warren 2015; Malik & Nazir 2012). Sweetman (2019) encourages decision-makers to verify if the enterprise uses highly classified or sensitive data which should not be stored, accessed, or transferred over an Internet connection. Decision-makers can organise data in relevant categories for easy use and effective protection if they understand data classification (De Groot 2019), which involves sorting out enterprise data into different categories, depending on characteristics, such as the level of sensitivity (Shaikh & Sasikumar 2015). This activity can enable decision-makers to identify the current data formats, the source of data, its sensitivity, and the expected format after migrating to the cloud (Khan & Al-Yasiri 2015; Anala, Shetty & Shobha 2013). This information is needed to identify possible vulnerabilities and risks to the data before migrating it and then decide which security measures an enterprise should take when migrating such data. De Groot (2019) argues that data classification can be content, context or user-based, which is important for both risk management and data security in cloud services. Simorjay (2014) views data classification as a means by which management can categorise data stored in their enterprise based on sensitivity and business impact to establish the risks associated with the data. Data can be classified as restricted, private or public to indicate its sensitivity and accessibility, which can be used to decide the type of protection suitable for each (Shaikh & Sasikumar 2015; Agostino et al. 2013). At the end of data classification, decision-makers will have a clear picture of all data which the enterprise has control over, including its location, ease of access and the most appropriate ways of protecting it from potential security risks. Checklist 1 is for use during the data classification stage at the beginning of the evaluation.

### iii. Assessing the security requirements for data to be migrated to the cloud

Due to the lack of security expertise in SMEs, decision-makers are discouraged from hastily migrating sensitive data to the cloud without enough knowledge about security requirements against cybersecurity breaches (Modi et al. 2013; Sen 2013). After data classification, the CBISEF suggests that decision-makers should assess the security requirements of each type of data based on sensitivity. The common practice is to secure sensitive or critical information from unauthorised access and disclosure by providing proper access control, encryption, and threat management (De Groot 2019; Schaefer et al. 2014; Tamer et al. 2013).

Decision-makers would be required to complete the respective section of Checklist 1 in *Figure AP6.1 in Appendix K* when assessing each of these criteria. Once decision-makers are aware of the security requirements of each type of data, they can assess security controls in the shortlisted Cloud BI.

### Cloud business intelligence usability and security assessment

This component of the CBISEF consists of six activities that decision-makers should undertake to assess a Cloud BI. Figure 6.6 shows the suggested activities and the expected output. Each of the activities can be assessed using Checklist 2 in *Figure AP6.2 in Appendix K*.



**Figure 6.6: Assessing different aspects of Cloud BI**

#### i. Identification of Cloud BI that match the business and data security needs of the enterprise

Due to the presence of many Cloud BI on the open web, decision-makers need to identify solutions that meet their business needs and data security requirements instead of handpicking one. This could be achieved by searching the open web for various free or low-cost Cloud BI, or by consulting friends or specialists for specific solutions (Gartner 2016; Salim et al. 2015; Hooda 2014; Moore 2014). A better way of identifying Cloud BI would be locating the current and most

popular applications (Pratt & Fruhlinger 2019; Izrailevsky & Bell 2018). A trial version can be used to assess each possible solution, carefully documenting the functionalities and other features that the enterprise considers necessary. The use of a checklist in assessing Cloud BI usability is recommended by Choi and Lee (2015). This research incorporated a section in Checklist 2 to assist SME decision-makers in identifying Cloud BI suitable for their enterprises.

## **ii. Assessing the functionalities of Cloud BI for key data management and security**

The identification and analysis of the basic functionalities of Cloud BI that an enterprise needs to meet data migration, processing, storage, visual displays, and security expectations (Koparkar & Mackrell 2015). This view is further emphasised by (Hussain et al. 2018) posit that enterprises need to ascertain whether the cloud services they intend to adopt will allow end-users to have access to the functionality of the application that they want to use and if they will continue to have access to the data, even if the access was removed. Pratt and Fruhlinger (2019) encourage clients to assess essential components of Cloud BI solutions, such as dashboards and visualisation tools used for reporting purposes. Checklist 2 has to be completed for these criteria.

## **iii. Assessing security vulnerabilities, threats, and risks in the shortlisted Cloud BI**

The CBISEF provides for the examination of security vulnerabilities, threats, and risks to data that can occur in each of the shortlisted applications. Studies suggest that relevant historical information about Cloud BI can be found from different sources, such as the web in the form of user reviews, other users, business partners, and CSPs (Salim et al. 2015, 2016). According to Sanjay and Vijayaraj (2011), an easy-to-use interface was likely to be vulnerable to many threats and present security risks to the data accessed by the application. This notion discourages decision-makers from relying on oversimplified interfaces because these tend to be vulnerable. Decision-makers have to assess how the Cloud BI integrate with existing IT solutions in the enterprise as this can be a security weakness. A threat risk profile for each Cloud BI can be compiled and used for comparison purposes. The assessment should consider the data security requirements, the security controls in place, and the type of cloud deployment to be used.

#### **iv. Assessing security controls in place and their robustness**

Data security and privacy are always cited as the biggest risks to enterprises who intend to migrate services to clouds (Elena & Johnson 2015b; Rivastava & Kumar 2015; Sen 2013). This is a key aspect of the evaluation process that decision-makers must emphasise to protect data at rest, in transit and being processed (Woodhead 2018). The CBISEF requires decision-makers to verify if each Cloud BI has operational security controls, such as access control (authentication and authorisation), data recovery, data encryption, business continuity plans, a backup facility, and anti-malware (Wu & Gusman 2019). According to Cohen (2019), Cloud BI must have security features and security capabilities that are compatible with other security features deployed on the distributed network. The assessment of access security controls should check for features that users can configure, such as requisite password changes, and automatic timeouts of sessions that are affected by shared security responsibilities with the CSPs (Gajajiva 2019; Information Security Forum 2016; Sen 2013; Subashini & Kavitha 2011). These controls should be assessed for their effectiveness in protecting unauthorised access to enterprise data and information stored in the cloud. The presence of security controls in the systems is not enough to guarantee security, hence the need to assess the robustness of those controls. Robust security is needed to assure better protection for the CIA when using IT assets (Canadian Centre for Cyber Security 2019). According to the Canadian Centre for Cyber Security (2019), robustness refers to the characterisation of the security strength and assurance of control, service, mechanism, or product. Decision-makers are encouraged to assess the strength of security controls in place to assure CIA and privacy when the Cloud BI is being used. Decision-makers can assess whether the security controls perform what they are designed for by using Checklist 2, Figure AP6.2.

#### **v. Assessing Cloud BI usability by non-technical users**

This is another aspect in the evaluation of Cloud BI that decision-makers indicated should be considered. Stanton and Theofanos (2018) argue that usability is the extent to which a system, product, or service can be used by certain users to meet the intended goals of effectiveness, efficiency, and satisfaction in each context of use. This requires decision-makers to check how user-friendly are the features of the Cloud BI to users with little technical knowledge of the system without breaching the system's security. Usability assessment extends to the effort that the user will learn how the system works and use without taking formal training (Stanton & Theofanos



2018; Rostek et al. 2012). Usability evaluation focuses on how well users can learn and use a product to achieve their goals (Horakova & Skalska 2013; Pant 2009). It refers to how satisfied users are with that process (Pratt & Fruhlinger 2019). Unlike business analytics, BI is descriptive and aims to provide simple snapshots of the current state of affairs to business managers and make it easy for non-technical end-users to understand how to process simple data by creating new reports (Pratt & Fruhlinger 2019; Devesh et al. 2017). Decision-makers would have to assess the level of training needed to use each shortlisted Cloud BI and the cost of such training. User-friendliness and the quality of the application in meeting the user expectations can be assessed using Checklist 2, Figure AP6.2

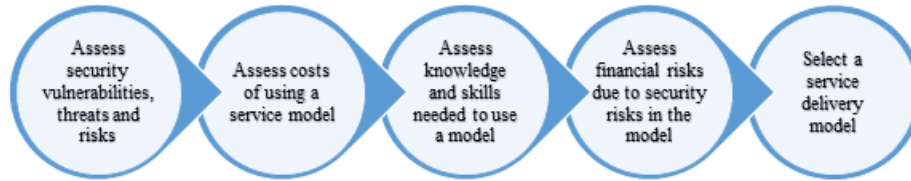
vi. **Assessing the cost and financial risks of each shortlisted Cloud BI solution**

Although some Cloud BI are free, they pose financial risks to the enterprises and must be assessed beforehand to avert negative effects on the profit and viability of SMEs. CSPs use different pricing models which SMEs must assess to avoid running into unnecessary costly financial risks (Morneau 2019; Indriasari et al. 2018). This means that decision-makers must analyse the items paid for in each Cloud BI. For the rented Cloud BI, decision-makers need to assess financial risks which may include contract modification or cancellation fees, the additional overhead of managing CSPs, and penalties for overuse of services (Gadia 2018; KPMG 2016; Tiwari & Mishra 2012). Decision-makers need assistance to understand and identify the components for which CSPs and vendors charge more. Checklist 2 in Figure AP6.2 is used to assess the usability and security of the Cloud BI.

**Cloud business intelligence service delivery models assessment**

Cloud BI is delivered over cloud computing service delivery models, mainly IaaS, PaaS and SaaS (Papachristodoulou et al. 2017; Phneah 2013; Lechesa et al. 2012). Several studies recommend that SMEs adopt Cloud BI offered as SaaS rather than IaaS and PaaS because SaaS provide much-improved security to data and applications they host for clients (Gajajiva 2019; Pratt & Fruhlinger 2019; Woodhead 2018). The choice of cloud service delivery models is essential in the adoption of Cloud BI because each service model presents different security challenges. Decision-makers need to be familiar with different service delivery models and understand how each relates to their data management and security schemes. Furthermore, decision-makers need to identify the most

appropriate cloud service delivery model which optimally addresses their business needs (Song 2013; Tamer et al. 2013). To select the appropriate service delivery model, the framework delineated four crucial activities that can be carried out, as shown in Figure 6.7. Each activity is assessed as a criterion using Checklist 3 in *Figure AP6.3 in Appendix K*.



**Figure 6.7: Service delivery model assessment**

**i. Assess security vulnerabilities, threats, and risks in a service delivery model**

There is a plethora of literature about security issues in each of the three service delivery models and this justifies the need for decision-makers to assess each beforehand (Dhar 2014; Harfoushi et al. 2014; Chen & Zhao 2012). Although SaaS is claimed to provide a more secure BI service than on-premise BI and other on-premise applications, the literature shows that it is prone to security breaches and requires evaluation (Gajajiva 2019; Wu & Gusman 2019). The assumption that SaaS providers are security specialists should not stop decision-makers from assessing security vulnerabilities in SaaS. Decision-makers can analyse security vulnerabilities, threats, and risks in each service delivery model, considering the type of Cloud BI selected and data security requirements. A comparison of security breaches in each service delivery model can be made. The study suggested that decision-makers use Checklist 3 in Figure AP6.3 to assess this aspect.

**ii. Assessing costs of using each service delivery model**

Cloud computing services are intended to reduce the cost of IT infrastructure and software and be accessible to the entire business enterprise (Iqbal et al. 2016). Decision-makers should assess the costs of using a given service delivery model to decide whether the enterprise's budget can sustain the adoption and use of the Cloud BI in that model. Literature shows that each service delivery model has cost implications for the enterprise and this requires an assessment before adoption (Dresner 2017; Elsanhoury, Ahmed & Abdullah 2012). Each type of cloud service delivery model suits certain business operations and potentially alters the security, controls, and costs that an enterprise is used to (Marquis 2018; Bamba 2012). The most appropriate service delivery model is the one that is more cost-effective and has better security features that decision-makers can easily

become familiar with. Service delivery models which require the hiring of technical security personnel are generally expensive and SMEs may not be able to afford the costs. According to Song (2013), cloud services should be evaluated by focusing on reducing risk and trading-off between performance and cost. Of the three service delivery models, studies recommend that SMEs choose SaaS if the enterprise relies on CSP Cloud BI or IaaS if the enterprise has its own BI to migrate to the cloud (Marquis 2018; Kumar & Padmapriya 2014). PaaS requires a degree of software development skills that decision-makers may not have and this can present another challenge for them (Chou 2013; Sen 2013). Decision-makers should be cognizant of the fact that they have very limited control over the Cloud BI hosted in SaaS, besides limited user-specific application configuration and settings (ENISA, 2015; Kumar & Padmapriya, 2014). This has cost implications for the enterprise, especially if a security breach occurs in SaaS, the CSP may apportion the blame on the enterprises.

### **iii. Assessing the knowledge and skills needed to use each service delivery model**

This aspect was found to be essential in the evaluation of Cloud BI. Different service delivery models require a different amount of effort, knowledge, and technical skills. Decision-makers must assess service delivery models considering the knowledge and skills required to use them. A service model which demands less technical knowledge and skills were ideal for SMEs. Service delivery models which require advanced technical skills are generally difficult to use by non-technical persons. According to Marquis (2018), decision-makers would need to assess their ability to acquire, provision, consume, and audit cloud services. Morneau (2019) recommends that the assessment of the time and effort needed to learn to use and manage different aspects of the cloud infrastructure before making a final decision is essential. This implies that decision-makers must evaluate Cloud BI in terms of new skills demanded of them, particularly for IaaS where they may be required to create, install, monitor, and manage platforms for services and applications. PaaS presents decision-makers with the challenges of developing, testing, deploying, and managing applications hosted in the cloud. Instead, decision-makers could opt for SaaS in which there is provisioning for full BI through the network or web. By assessing the level of skills and knowledge needed to use the service models in place, decision-makers will be able to recommend the one which requires limited financial resources for training purposes.

#### iv. Assessing financial risks due to security risks in each service delivery model

Besides, the costs of services and training, decision-makers need to assess financial obligations arising from data breaches because of the service delivery model used. Marquis (2018) posits that cloud services bring about benefits as well as risks. Enterprises should identify and find ways to mitigate these risks before adoption. In this context, decision-makers use Checklist 3 in Figure AP6.3 to assess the service delivery models.

#### Cloud deployment models assessment

The presence of multiple cloud deployment models to select from necessitates the assessment of the suitability of each model according to the scheme shown in Figure 6.8. The main aspects to be assessed include security vulnerabilities, threats and risks, costs of using the cloud, and possible financial risks which may be caused by data breaches, litigation, and loss of business. Although decision-makers may have cloud deployment model preferences, they are encouraged to be familiar with each of the common models to understand the data security issues, risks, and investment opportunities that each presents (FindLaw Attorney Writers 2018; Kelley & Warren 2015). Checklist 4 in *Figure AP6.4 in Appendix K* was recommended for use in assessing this component.



**Figure 6.8: Cloud deployment model considerations**

#### i. Assessing vulnerabilities, threats, and risks in each deployment model

The Cloud adoption evaluation process requires that decision-makers identify and decide which enterprise IT infrastructure will be integrated with the Cloud BI. Bamba (2012) views Cloud BI as a form of SaaS BI at a lower cost intended for quicker implementation with more improved scalability than traditional BI and insists that they can be integrated with on-premise systems. According to Yauri and Abah (2016), on-premise infrastructure that will be integrated with cloud applications needs to be more secure to prevent unauthorised access and infection by malware over the internet or web. Morneau (2019) suggests that enterprise managers should assess the ease with which the selected Cloud BI integrates with their existing systems and the support offered by the

CSP. Security vulnerabilities, threats, and risks to the infrastructure are assessed together with the corresponding deployment models. Decision-makers can use Checklist 4 to assess these key aspects of Cloud BI.

**ii. Assessing the effectiveness of security controls in place**

Enterprise decision-makers need to be aware of security controls deployed by the CSP in each cloud deployment model so that they assess their effectiveness in preventing and mitigating data security breaches and risks (Marquis 2018; Bamba 2012). This is intended to assist decision-makers in understanding how security controls work and what needs to be improved. For the public cloud, the assessment of data segregation, hacking, and data recovery needs to be done as a security measure to enterprise data before migrating to the cloud. Decision-makers should check that the Cloud BI allows only authorised users to have access to the systems. The effectiveness of the security controls in protecting data in the cloud needs to be assessed in terms of CIA, privacy, and the consequences if these are not provided for. This allows the decision-makers to prove the claims made by CSPs about the security of the cloud models provided.

**iii. *Assessing the availability, reliability, and performance of cloud deployment models***

The assessment of the availability of services in each cloud deployment model is essential to the enterprises. Decision-makers should know the times that the data centre will be accessible to deliver the expected IT service proportional to the cost of services (Raza 2018). Availability ensures successful connectivity to the cloud for authorised users who need to use the systems or network (Ziglari & Negini 2017). According to Mesbahi, Rahmani and Hosseinzadeh (2018), CSPs face challenges in providing dependable cloud environments that match the needs of cloud users. This compels decision-makers to assess the availability, reliability, and performance of the cloud deployment model before adopting it. Decision-makers should ascertain the frequency of downtime of the service to determine the availability of the cloud. Cloud reliability means that users should have timely access to data and mission-critical services occurring in the cloud without failure during all the times agreed upon in the contracts (Izrailevsky & Bell 2018; Harfoushi et al. 2014; Bills 2012). Assessing the reliability of the cloud enables decision-makers to understand how well the Cloud BI would fare under different conditions that they want to use it (Raza 2018). The CloudHealth Tech Staff (2018) recommends that cloud users assess the reliability of the cloud

in terms of security, connectivity, and performance. Decision-makers need to have a basic understanding of the quality of service of the cloud by assessing the performance of the cloud. This can assist decision-makers to ascertain whether the cloud system works properly, and the connectivity is available and reachable whenever the user needs it (CloudHealth Tech Staff 2018; Izrailevsky & Bell 2018; Mesbahi et al. 2018; Raza 2018). The use of Checklist 4 can assist decision-makers to assess this aspect.

#### **iv. Assessing cloud interoperability and application portability**

The findings of the study show that decision-makers were concerned with the interoperability and portability of their data and application to be migrated to the cloud. These fears can be dispelled by assessing cloud interoperability and data portability to determine how easy and safe it is to move data from the on-premises to the cloud and back or from one cloud to another. Rezaei et al. (2013) argue that poor interoperability between two different systems can be a major security challenge of data availability for the users. This implies that decision-makers need to be certain that the interoperability between enterprise systems and the Cloud BI is acceptable according to their needs. The knowledge about cloud interoperability is important for decision-makers because different CSPs use different technologies in their cloud infrastructure, platforms, and software (Cloud Standards Customer 2017; Novakouski & Lewis 2012). The purpose of assessing interoperability and portability is to avoid data lock-in (Opara-Martins et al. 2016; Fitzpatrick & Lueck 2010). To avoid the possibility of vendor lock-in, decision-makers should assess the extent to which each shortlisted CSP uses proprietary technology (Cloud Industry Forum 2019; Cloud Standards Customer 2017). The CSP using minimal proprietary technologies should be preferred, as this reduces interoperability challenges (Opara-Martins et al. 2016). When selecting Cloud BI, potential adopters are encouraged to assess the ease with which data and application components can be moved and reused in different clouds, irrespective of the CSP, platform, operating systems, infrastructure, location, storage, the format of data, or APIs (Rivastava & Kumar 2015; Hooda 2014; Kumar & Padmapriya 2014; Rostek et al. 2012; Cloud Security Alliance 2011). Assessment of data portability can assist decision-makers in verifying the compatibilities between on-premises and Cloud BI to prevent data corruption during the conversion processes. A provision to assess this aspect is made in Checklist 4, Figure AP6.4.

#### v. **Assessing costs of the deployment model**

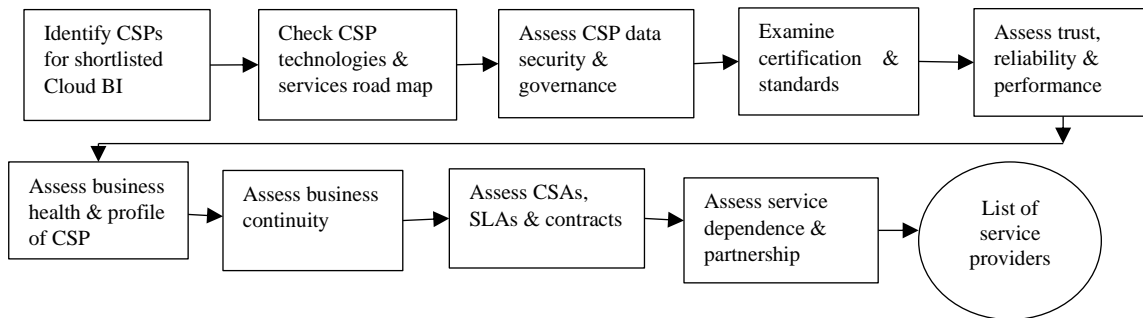
The purpose of using cloud technologies is to reduce the cost of IT investment while increasing business viability through good decision-making (Choi & Lee 2015; Rostek et al. 2012). Cloud deployment models vary in their costs, and this needs to be assessed to enable the enterprise to select one that it can afford. The cost of the cloud enables potential users to decide whether to use a public, private, community or hybrid deployment model (Marko 2018; Song 2013). Due to financial constraints, SMEs prefer low-cost public clouds to private ones (Devesh et al. 2017; Ngeru & Bardhan 2015). However, public clouds offered by different providers need to be assessed, as they are not priced uniformly. Marko (2018) posits that the cost assessment of cloud deployment models involves different aspects for different deployment models, making it a challenge to attain. Sweetman (2019) encourages decision-makers to assess if the cost of the cloud business solution is aligned with business strategy and budget constraints. This study suggests that decision-makers get an itemised electronic invoice from different potential CSPs meeting the other criteria used and use Checklist 4 to assess the costs involved.

#### vi. **Assessing the financial risks of using the deployment model**

According to Sweetman (2019), public cloud deployment models have benefits in the form of easy to configure, easy data access, high scalability, cost-effectiveness, and assured availability due to continuous maintenance by CSPs. However, the author highlights disadvantages emanating from high-security risks due to ever-increasing cyber threats which exploit inherent security flaws, privacy breaches, reliability issues, and lack of customisation or individuality. This requires decision-makers to assess the financial risks that an enterprise can suffer due to the negative aspects of the public cloud. The private cloud deployment model has greater control over enterprise data, improved security, privacy, and dependability but are costly due to high financial investments in hardware, software, and infrastructure and the high degree of training to run the model (Sweetman 2019; Marko 2018; Agrawal, Abbadi & Wang 2011). Decision-makers need to assess financial risks that may arise due to security risks and the acquisition of infrastructure they may not be able to use, due to high skill and knowledge demand. These are attributes that the TPB, DoIT and TAM allude to when considering adopting technologies.

## Assessment of cloud service providers

The findings of the study indicate that decision-makers did not trust CSPs in various aspects, particularly security provision, contract honouring and provision of promised services. Furthermore, decision-makers recommended assessing CSPs when evaluating Cloud BI to select the most appropriate one. Figure 6.9 shows the aspects of CSPs that decision-makers can assess during the evaluation process and *Checklist 5 in Figure AP6.5 in Appendix K* can be used to assess each of the suggested aspects.



**Figure 6.9: Cloud service provide assessment and selection**

### i. Identify possible CSPs for shortlisted Cloud BI

Currently, the selection of the most appropriate CSPs is complicated by the lack of a common assessment framework and differences in what the CSPs use (Lacey and James, 2010; Cloud Security Alliance, 2016; Morneau, 2019). According to Morneau (2019), Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Services (GCS) are the major international CSPs who have established local cloud services that local business communities can select from. Apart from these three big CSPs, there are some local CSPs from which different SMEs can select. Decision-makers would have to identify CSPs who provide the appropriate deployment and service delivery models for the preferred Cloud BI and match the business, operational and security needs of the enterprises. Alternative sources for decision-makers include the web, IT specialists, and friends in the same business or services. This task imposes a challenge on decision-makers as they may have to evaluate numerous CSPs. However, some authors recommend that SMEs start with famous local CSPs, in this case, South African ones, before looking at international ones. Checklist 5, in Figure AP6.5, can be used by decision-makers to identify appropriate CSPs.



## ii. **Check CSP technologies and services roadmap**

Due to the presence of many CSPs in the market, decision-makers are encouraged to check whether the platform and technologies offered by a service provider support their cloud objectives and fit with the existing enterprise operational environment (Cloud Industry Forum 2019). This enables decision-makers to determine whether the enterprise can be forced to buy new technologies to replace the existing ones and the financial implications that this has on the budget, especially if they have to buy additional equipment. Besides financial issues, acquiring new technologies places additional demands on knowledge and skills that decision-makers should have to use the systems. This implies that decision-makers need to understand the commitments to particular technologies by CSPs and vendors and how they support interoperability and data migration (ISACA 2011; Hashizume et al. 2013). By assessing individual CSPs, decision-makers will be able to determine which cloud architectures, standards and services match the enterprise's workloads and management preferences (Cloud Industry Forum 2019). For public clouds, decision-makers should verify whether the CSPs provide data segregation for safe operations in a multitenant environment (Ramachandran & Chang 2016; Youssef & Alageel 2012; Ramgovind, Eloff & Smith 2010). The assessment of CSP technologies will make decision-makers understand the migration services, assistance, or support being offered and the role that the enterprise will play in the adoption process (Opara-Martins et al. 2016; Kelley & Warren 2015). According to the University of Leicester (2015), assessing the CSP is essential for decision-makers to ascertain whether the cloud technologies being offered will enable the enterprise to grow in the direction predicted in the strategic plan. Checklist 5 provides for the assessment of this aspect.

## iii. **Assess data governance and security**

In this aspect, decision-makers need to consider how the CSPs manage the different types of data and the security provided. The assessment should focus on the ability of CSPs to perform complete data recovery and system restoration when a disaster occurs. It is recommended that decision-makers assess the levels of data security, system security, the maturity of security operations, and security governance processes. Decision-makers should understand the security goals of their enterprises and the security measures each CSP offers to preserve applications and data in the cloud (Niselow 2018; Symantec Corporation 2014). Security controls used in the cloud should be observed to identify whether they support enterprise security processes and policies (Vacca 2017;

The University of Leicester 2015). Decision-makers are supposed to get clear explanations on the security roles and responsibilities provided in the contracts, policies, or SLAs, beyond the ability of the CSP to ensure user access and auditing of activities over the network (Vacca 2017; Shimamoto 2015). Studies recommend that decision-makers make formal requests for CSPs' security audit and incident reports as well as proof of a corrective measure that was taken to address the security breaches reported (Jakimoski 2016; Cloud Security White Paper 2011). Additionally, the assessment of security should target the available tools for data backups from the cloud to a storage facility selected by the enterprise. Checklist 5 can be used to accomplish this.

#### iv. **Examine certification and standards**

One of the most reliable and recommended ways to assess whether CSPs adhere to standards and best practices in the industry is through their compliance with the well-known standards and quality frameworks (Soong & Lam 2015; Agostino et al. 2013; Youssef & Alageel 2012). According to the Cloud Industry Forum (2019), CSPs should be assessed for compliance with standards, such as ISO 27000 series, or whether they possess recognised and valid certifications. Decision-makers can request CSPs to provide proof of their certifications which prove validity and compliance with industry standards. As for industry standards, decision-makers can find them on the web. Morneau (2019) encourages SMEs to choose CSPs who provide platforms that assist enterprises to be compliant with industry standards relevant to their business industry. Certifications and standards stipulate the requirements that CSPs and enterprises should adhere to, to attain best practices for information security management (Cloud Standards Customer Council 2016; Tofan 2011). CSPs who meet the standards and expected quality of the framework are reported to be eager to show clients proof of compliance with the industry's best standards and practices (Cloud Industry Forum 2019; Tofan 2011). Decision-makers are expected to verify whether CSPs adhere to common standards and certifications.

#### v. **Assessing security, trust, reliability, and performance**

Enterprises intending to migrate to the cloud expect CSPs to be trustworthy in keeping their data safe while providing services as agreed in the SLAs. This suggests that decision-makers must assess CSPs' trustworthiness and reliability in service provision and performance. Reliability can be assessed by checking the performance of CSPs against their SLAs for a year and the information

can be obtained from publications or on request by clients (Cloud Industry Forum 2019). In this study, decision-makers can check the frequency of downtime and how the CSPs deals with it, and whether the processes of tackling both planned and unplanned downtime were documented and approved as recommended by Mesbahi, Rahmani and Hosseinzadeh (2018) and Stanton and Theofanos (2018). The reliability of a CSP depends on the agreement of the availability of the services for a given percentage, during specific hours, determined by the duration of time agreed upon (Behr 2017; Foley & Lardner 2015). This would include checking how CSPs implement data and application recovery and compensate the client for lost businesses due to system unavailability.

**vi. Assessing business health and profile of CSP**

Potential CSPs should not only meet technical, security and operational expectations of the client enterprises but should be financially sound with a health profile to sustain the long-term survival of their business entity (Cloud Industry Forum 2019). According to Mesbahi, Rahmani and Hosseinzadeh (2018), a good CSP should have a stable track record supported by good financial and capital standing for long term survival. Assessing the business health and profile enables decision-makers to identify CSPs who have financial problems and are likely to close down shortly. This would assist enterprises in avoiding future security challenges such as data lock-in and financial risks from hidden costs (Mesbahi et al. 2018). Decision-makers are encouraged to check the pending financial obligations of CSPs, such as litigations and outstanding refunds. Information about a CSP can be obtained from discussion boards or social media forums, such as LinkedIn, where potential users meet.

**vii. Assessing business continuity**

Enterprises adopt technologies to improve their operations through good decision-making. To benefit from Cloud BI, decision-makers need to assess business continuity. Conducting background checks on CSPs prevents the hosting of enterprise data and applications by CSPs not able to attend to system disruptions or outages, not able to provide business continuity, or who engage in malicious or fraudulent activities (Schaefer et al. 2014; Vohradsky 2012; ISACA 2011). Foley and Lardner (2015) recommend that enterprises request CSPs to demonstrate and promise the ability to provide the services in the event of a disaster, power outage, or significant adverse

event. Decision-makers who lack confidence in the financial stability of CSPs should assess the readiness of the provider to make financial conditions available to determine beforehand whether services will continue (Behr 2017; Foley & Lardner 2015; Greene 2010).

#### viii. **Assessing cloud service agreements and contracts**

It is recommended that decision-makers assess cloud service agreement (CSA) components, namely the acceptable use policy (AUP), customer agreement, and SLA (Behr 2017). Decision-makers need to understand CSAs which clarify service delivery, data policies and protection, business terms, legal protection, and SLAs from the CSPs (Cloud Security Alliance 2013; Greene 2010). These are some of the challenges that decision-makers highlighted that prevented them from adopting Cloud BI. CSPs are reputed to use jargon which makes contracts and SLAs very complex for ordinary IT users who want to adopt the solutions (Cloud Industry Forum 2019). According to Brebner and Liu (2010), CSPs offer SLAs which are weak and limited in scope and do not guarantee the availability of all resources and services promised. Behr (2017) posits that although CSAs, SLAs, and other contracts can range in their degree of complexity, enterprise decision-makers should take time to evaluate them to avoid financial risks. When evaluating CSAs, SLAs, and contracts, decision-makers should clarify their responsibilities and those of the CSP in data security, what should be negotiated, how to terminate the contract, and financial implications. In SMEs, decision-makers are responsible for ensuring that the Cloud BI to be adopted meets the needs, and it is up to them to consult with an IT specialist regarding contracts and technical matters covered in CSA and SLAs (Behr, 2017). During the assessment process, decision-makers must check if they have the right to terminate the contract when the CSP faces bankruptcy and whether the CSP would assist the enterprise in migrating to another provider on termination or expiration of the contract or agreement (Foley & Lardner 2015). To deal with issues of mistrust, decision-makers can research the history of service provision of a CSP, particularly regarding additional hidden costs, dealing with overdue payments, and adhering to contracts in terms of services provided. Assessment of SLAs can provide decision-makers with key information about service levels and acceptable thresholds of service delivery by CSPs in terms of performance, uptime, and serviceability (Behr 2017). These can be assessed using a tool such as Checklist 5.

ix. **Assess service dependence and partnerships**

A CSP can depend on several vendors for infrastructure, software, and services. Decision-makers need to understand the relationships of CSPs and vendors concerning accreditation levels, technical capabilities and staff certifications, and support provided (Cloud Industry Forum 2019; Cloud Standards Customer 2017). By assessing CSP and vendor relationships, decision-makers would be in a position to identify service dependencies and understand the implications, responsibilities, and accountabilities of adopting Cloud BI (Behr 2017; Cloud Standards Customer 2017). Decision-makers should have an insight into the limitations of liability and service disruption policies due to service dependencies of each CSP and the financial risks involved. To trust a CSP, decision-makers should be able to determine the direct responsibilities of the former to compensate for the losses incurred by the enterprise, without engaging in complexities involving several vendors. Checklist 5 shown in Figure 6.14 was designed to assess the CSPs during the evaluation process.

**Financial risks assessment**

Financial risks have emerged as the most popular factor preventing enterprises from adopting and using Cloud BI. Findings indicate that financial challenges preoccupy decision-makers throughout the evaluation process, although there was a clear awareness of the benefits of using Cloud BI and other cloud services. Figure 6.10 indicates the key activities of financial risk that decision-makers indicated should be assessed during the evaluation. Checklist 6 in *Figure AP6.6, Appendix K* is designed to assess the components of financial risks.



**Figure 6.10: Financial risks assessment**

i. **Assessing hidden costs**

The use of Cloud BI can cause the enterprise to pay for extra or hidden costs not budgeted. Decision-makers need to assess the likelihood of paying hidden costs which CSPs can charge without the knowledge of their clients. According to Brey (2019), hidden costs are more prevalent

in the public than in other cloud deployment models. To avoid hidden costs, enterprises are encouraged to assess important types of services available, including on-demand, reserved or spot instances, such as the relevant storage, networking, and security required, if they match the enterprise workload, requirements, and expectations (Brey 2019; Staten 2013). Literature shows that some CSPs pretend to offer free assistance to clients and later charge at the expiry of the trial period or when the client decides to move the data and application out of the cloud to another CSP (Brey 2019; Bignel 2017). CSPs achieve this by making the initial subscription free or low to lure unsuspecting potential clients and then increases sharply after the trial period or after adoption (Brey 2019). Due to this unethical practice by CSPs, decision-makers need to verify that shortlisted CSPs do not factor in hidden costs. Durcevic (2019) highlights that using proprietary Cloud BI usually leads to hidden costs through hiring technical experts to assist in data migration or writing code in the event of incompatibilities occurring between data and Cloud BI. Checklist 6 can assist decision-makers in assessing possible financial risks emanating from hidden costs.

#### **ii. Assessing costs due to downtime**

The National Computing Centre Group (2018) regards cloud service downtime as a top concern for enterprises and one of the major reasons for customers not willing to adopt and use cloud-hosted software. Enterprises using Cloud BI depend on CSPs for most of the business transactions and can suffer financial risks if the service is down, unavailable or unreliable (Durcevic 2019). According to Durcevic (2019), the performance of a Cloud BI on an enterprise depends on the performance and reliability of the CSP, therefore client enterprises should guard against paying for poorly performing CSPs. Decision-makers should check that CSPs have mechanisms to compensate for outages, particularly for pay-as-you-go services. Drye and Warren (2015) opine that decision-makers should understand how service interruptions affect the availability and accessibility of data stored in the cloud and then assess any liability if an enterprise fails to have access to data on the cloud. It is suggested that SLAs be assessed for disclaimers on unauthorised data access and hacking and the level of security provided to enterprise data in the cloud to cater for possible data breaches (Claycomb 2012; Robinson et al. 2010).

### iii. **Assessing litigation costs**

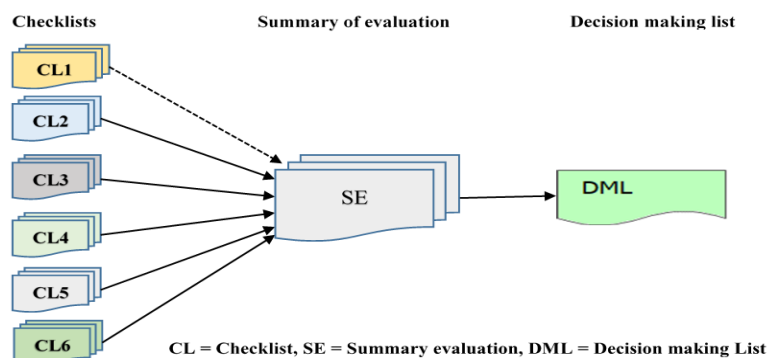
These are unexpected costs that arise from noncompliance by both CSP and client enterprises that attract litigation by customers or penalties by governments in the country where the data is hosted (Durcevic 2019; Cloud Security Alliance 2016; Akinbi 2015; Pearson & Benameur 2011). Regardless of the best measures put in place by CSPs, enterprises can end up paying expensive lawsuits for failing to protect sensitive customer information from cybersecurity threats that breach privacy (Koops & Goodwin 2014; Raza 2013). This implies that legal issues which are likely to hamper the adoption and beneficial use of Cloud BI and other cloud services should be meticulously assessed before an enterprise migrates its business functions to the cloud (Tembedza 2012). Decision-makers should research various cloud offerings to ascertain that CSPs' services meet the needs of the enterprises or cross-border transfer restrictions and requisite security controls (FindLaw Attorney Writers 2018; Tembedza 2012). According to Kelley and Warren (2015), the selection of the cloud deployment model should be based on the type of data to be stored in the cloud, as well as the legal obligations the enterprise has on that data. Decision-makers need to know the financial penalties the enterprise would incur when it violates stipulated threshold policies. Foley and Lardner (2015) encourage enterprises to check that there is appropriate contractual protection for different security and financial risks emanating from service unavailability when assessing CSPs.

### iv. **Assessing penalty costs for misuse of services**

An enterprise is expected to comply with regulations and standards regardless of where the data are stored. Failure to do so can lead to penalties by CSPs or local authorities (Brey 2019; Durcevic 2019; Bignel 2017; Romes 2015; Greis 2014). The enterprise must assess the potential penalties that result from non-compliance and not turning off some services that are not in use (Staten 2013). When using a trial version, decision-makers need to assess the costs of leaving the cloud without suffering financial loss (Raza 2013). According to Raza (2013), enterprises would have to assess the cost of support provided by the CSP when there is something to be resolved in the cloud. Checklist 6 has a section to assist decision-makers to assess financial risks when evaluating Cloud BI.

#### 6.2.4. Using the checklists in the evaluation process

The evaluation process begins with a decision-maker completing Checklist 1, which requires the assessment of the preparedness of the enterprise to adopt and use Cloud BI. Figure 6.11 depicts the layout of how the evaluation process of six components would proceed and the completion of the checklists (CL1 to CL6), summary evaluation sheets (SE) and decision-making list (DML). A checklist for use in each step is provided in *Appendix K*. Each component consists of activities that each decision-maker should perform with the aid of checklists (activities described in the previous subsections of this Chapter).



**Figure 6.11: Layout of the evaluation process**

CL1 can be completed once while CL2 to CL6 can be completed for the assessment of each Cloud BI application made. Decision-makers examine existing data management processes and the business objectives based on the assessment criteria and score each of them. The other five checklists are completed sequentially depending on when the minimum actual percentage for the current component is met. The summary for each completed evaluation is recorded in a summary evaluation sheet shown, (*see Table 6.1*).



**Table 6.1: Summary evaluation sheet**

| Cloud BI Name:.....   |   |                |              |          |                    |               |               |
|---|---|----------------|--------------|----------|--------------------|---------------|---------------|
|   | COMPONENT ASSESSED  | Expected Score | Actual Score | Actual % | Minimum expected % | Decision      |               |
|   |   |                |              |          |                    | Accept        | Reject        |
| 1   | Business needs and data security requirements in the cloud  | 17             |              |          |                    | Accept        | Reject        |
| 2   | Cloud business intelligence application usability           | 25             |              |          |                    | Accept        | Reject        |
| 3   | Assesses service delivery models                            | 16             |              |          |                    | Accept        | Reject        |
| 4   | Cloud deployment models                                     | 17             |              |          |                    | Accept        | Reject        |
| 5   | Cloud service provider's trust, reliability and performance | 32             |              |          |                    | Accept        | Reject        |
| 6   | Assessment of financial risks                               | 20             |              |          |                    | Accept        | Reject        |
| <b>NB: Final decision: Accept if all accept; reject for at least one component with a reject decision</b> |   |                |              |          |                    | <b>Accept</b> | <b>Reject</b> |

To decide whether to adopt a Cloud BI, the actual percentage and minimum expected percentage for each component are compared. If the actual percentage is greater than or equal to the minimum expected percentage, the component is provisionally accepted by the Cloud BI; otherwise, it should be rejected. The Cloud BI is accepted if the decision for all components is *Accept*. For better comparison of results and decision-making purposes, the decision-making list, Table 6.2 is completed with information from the summary evaluation sheet of each assessed Cloud BI.

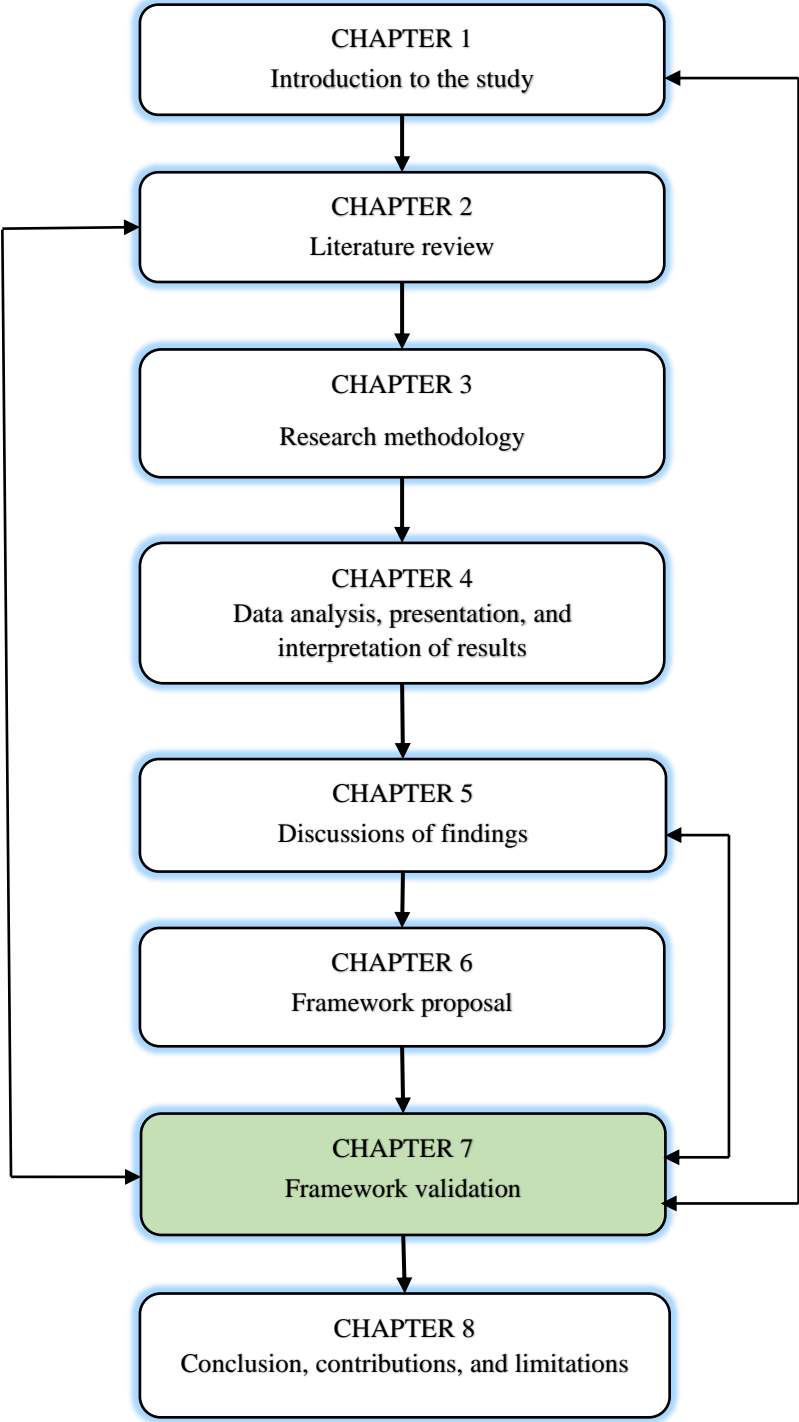
**Table 6.2: Decision-making list**

|    | Name of Cloud BI | Scores (%) |                  | Decision |        | Reasons | Date | Signature |
|----|------------------|------------|------------------|----------|--------|---------|------|-----------|
|    |                  | Actual     | Minimum expected | Accept   | Reject |         |      |           |
| 1. |                  |            |                  |          |        |         |      |           |
| 2. |                  |            |                  |          |        |         |      |           |
| 3. |                  |            |                  |          |        |         |      |           |
| 4. |                  |            |                  |          |        |         |      |           |
| 5. |                  |            |                  |          |        |         |      |           |
| 6. |                  |            |                  |          |        |         |      |           |

### 6.3. Conclusion

This chapter proposed a security evaluation framework for Cloud BI that could be used by SME decision-makers who have limited IT security knowledge and skills to evaluate Cloud BI. The framework consists of six components identified from the findings of the empirical section of this study. The chapter critically analysed the CBISEF by using a simple flow diagram and checklists that novice users can use in the evaluation process. The framework emphasises reducing financial risks, which SMEs were fearful of, by ascertaining that the Cloud BI were secure and provided by trusted and reliable CSPs who comply with industry standards.

**CHAPTER 7      FRAMEWORK VALIDATION**



## 7.1. Introduction

The previous chapter presented and analysed the security evaluation framework for Cloud BI based on the findings of the study. Samples of checklists to aid the evaluation process were presented for each component to be evaluated. This chapter provides a detailed validation of the CBISEF and checklists applicability among various SMEs in the selected towns in the Limpopo Province

## 7.2. Framework validation

After proposing the framework, validation was undertaken to ascertain whether the CBISEF reflected what decision-makers in SMEs expressed and its potential usefulness. The validation provided an answer to the SRQ5: *What did decision-makers consider to be the main components of the security evaluation framework for Cloud BI by SMEs?* The validation process provided an opportunity to present the proposed framework for scrutiny by IT security specialists and SME decision-makers who provided the basic ideas used.

According to Radatz, Geraci and Katki (1990), validation refers to the process of evaluating a system and its components, during or at the end of the development process, to ascertain if it meets the specified requirements. Similarly, Rykiel (1999) regards validation as a means to determine whether a framework is acceptable for its intended use and that it meets specified enterprise performance requirements. Validation is an important requirement of ISO 9000, used to ascertain the quality of a new application model or framework in terms of reliability, credibility, and usability in its applicable area (Kit 1995). This implies that validation was used to demonstrate that the framework met a satisfactory range of correctness for its intended application by SMEs (Kit 1995; Sargent 1984). However, Rykiel (1999) advises that a framework should be judged more for its usefulness than validity. This means that researchers should not be confined to justifying the complete reality or proving that the framework is the best available one, but strive to make its conceptual content acceptable to experts and users (Rykiel 1996). According to Sargent (1984), a credible framework is one in which a user has sufficient confidence to base scientific and management decisions. Consequently, in this study, credibility is used. Credibility has an adequate degree of acceptance in the validation of CBISEF, which justified its use for security evaluation and decision-making among SMEs. Literature shows that credibility has the advantage of being relative to a particular context of the framework and the amount of knowledge available, the

purpose of the framework, and the risks of any decisions made from using it (McLeod 2013; Rykiel 1996; Kit 1995).

In this study, content and face validity were used as relevance and acceptance validation techniques of the CBISEF, by IT security specialists and SME decision-makers.

### **7.2.1. Content validity as framework relevance validation**

Content validity is usually used to evaluate the extent to which a model or framework's components represent a real solution to the security evaluation problem (Al Nadab 2017; McLeod 2013; Müller & Roodt 2013). In this study, content validation involved assessing the relevance and applicability of the framework in the context of SMEs (Müller & Roodt 2013) and was achieved with input from IT security specialists in different organisations in South Africa. Content validity involved gathering evidence to support the relevance of the framework in the form of expert judgments about the components of a defined use (Krippendorff 2013; McLeod 2013). Studies show that content validation involves defining a domain, identifying the features of items to be reviewed, structuring the review process, selecting qualified experts, and collecting and summarising the data from their judgments (Crocker 2015). Relevance validation was conducted following Yusoff (2019), who advocates a sequence of steps that involve preparing a content validation form, the selection of a panel of experts for reviewing, performing content validation, reviewing area and items, allocating a score on each item, and calculating the content validation index.

### **7.2.2. Face validity as framework acceptance validation**

Face validity was conducted with IT security specialists and SME decision-makers to determine whether the CBISEF was a close, reasonable imitation of a real-world system they expected to have for evaluating Cloud BI. In face validity, it is recommended that knowledgeable people be asked if the model and its behaviour are reasonable (Al Nadab 2017; Müller & Roodt 2013). The purpose of face validity was to verify if the framework logic and input-output relationships had acceptable face-value regarding its use (McLeod 2013; Sargent 2011). In this study, face validity was conducted to establish the acceptance of the CBISEF by its intended users. According to

Krippendorff (2013), face validity is tested by asking experts, users, and other people with knowledge in the domain field in which the model or framework will be used, to identify its strengths, usability and deficiencies.

### **7.2.3. Purpose of validating the security evaluation framework**

The purpose of the validation process was to determine whether:

- i.* the CBISEF reasonably addressed the expectations of the decision-makers in SMEs of the selected towns;
- ii.* the CBISEF covered the major aspects to be evaluated in Cloud BI by SMEs;
- iii.* the CBISEF addressed key aspects of conventional frameworks such as COBIT, ISRM, NIST, ISO/IEC 2700 Series and ERM, which SMEs were not able to implement directly;
- iv.* the content of each checklist supported the CBISEF components;
- v.* the checklists were simple to understand and implement by SME decision-makers;
- vi.* the checklist statements addressed the required aspects of the framework; and
- vii.* the language used was appropriate for decision-makers with limited IT security.

## **7.3. Methodology**

A quantitative research design method was used in the validation processes. This involved the use of a cross-sectional survey in which two data sets, one for content validity and another for face validity, which was collected from different samples by employing two separate online questionnaires. Data for content validity was collected from a sample of IT security specialists and for face validity from both IT security specialists and SME decision-makers.

### **7.3.1. Validation instruments design and testing**

This part of the study used a panel of IT specialists and SME decision-makers to validate the content of the framework using online survey questionnaires. Two questionnaires, one for content (relevance) validation and the other for face (acceptance) validation, were designed from the six components of the framework and checklists. The relevance validation questionnaire consisted of 37 items from the six components of the CBISEF and were meant to test the acceptance of the

framework. This validation focused on establishing whether the components and checklist items were representative of the evaluation process to be performed by the CBISEF when used by decision-makers (Crocker 2015; Müller & Roodt 2013; Carson 2002). The online questionnaire was completed by 19 IT security specialists and 5 functional security experts in the assessment of the CBISEF.

The second questionnaire, for face validity, consisted of 30 items based on the six components of CBISEF and seven checklists. The questionnaire assessed whether the framework was acceptable, dependent on the reasonableness of its implementation for decision-makers. The respondents were asked to assess the logic of the framework and its relationships with checklists used for its implementation as suggested by Carson (2002), Sargent (2011), Krippendorff (2013), Müller and Roodt (2013) and Crocker (2015).

Each questionnaire provided clear guidelines of the task for each reviewer, the context of the problem, a brief description of the framework and checklists, rating scales of relevance for content validation, and acceptance for face validity. The questionnaires were piloted with three IT specialists and two decision-makers to correct the content language and remove repetition as recommended by Yusoff (2019). Corrections were made to the online questionnaires which were then emailed to a convenient sample of 20 IT security experts for relevance validation while the questionnaire for acceptance validation was emailed to 20 IT personnel and 24 SMEs for face validity.

### **7.3.2. Population, sample, and sampling procedures for framework validation**

Two target populations were used at the stage of validation, namely, IT security specialists for content validation and decision-makers of SMEs, who were using IT systems to support business operations, for face validation. The target population for IT security specialists included all accessible IT security specialists purposively sampled across South African provinces, who were readily available to complete the research instrument. The accessible population of decision-makers consisted of all SMEs in the five selected towns of the Limpopo Province who were currently using IT to support business operations. Due to the unavailability of the exact number of SMEs using ITs in the province, it was difficult to use a sample frame and therefore, the study

adopted a convenience sampling technique of those who participated in the original data collection process.

### **7.3.3. Data collection techniques**

Two weeks before data collection, the researcher emailed copies of CBISEF activities and the checklists to the respondents to inform them to familiarise themselves with the tools and the evaluation process. The respondents then completed the two online questionnaires following the instructions given. The data was automatically populated in different Google sheets which were downloaded at the end of the collection period of three weeks (15 June to 24 August 2020).

### **7.3.4. Data analysis techniques**

Data were analysed quantitatively, using SPSS producing correlation analysis for relevance validity, descriptive statistics, and Chi-square tests for acceptance validity.

## **7.4. Results of framework validation**

The results for validation are presented and interpreted in two sub-sections: Subsection 7.4.1: Content (*relevance*) validation; and 7.4.2: Face (*acceptance*) validation

### **7.4.1. Relevance validity**

Demographic information for the panel of reviewers for relevance validation is shown in *Table AP7.1, in Appendix L*. The results show that the reviewers for content validation consisted of IT security specialists with educational qualifications, namely, Bachelor of Science and Master of Science in Computing. Most of the reviewers, 78.9%, indicated that they had been in the IT industry for an average of five years, with good knowledge in Cloud business intelligence and other cloud services evaluation. Seventy-seven per cent of the reviewers had good to very good knowledge in security evaluation of cloud services and 94.7% had previous experience in reviewing security in IT systems and models. Based on this background information, these reviewers were deemed suitable to validate the relevance of the framework.

To validate the relevance of the CBISEF, the reviewers used a 4-point Likert scale in nine major categories of issues addressed by the framework (very relevant = 4, relevant = 3, moderately relevant = 2 and not relevant =1). The initial step focused on the relevance of the 6 components of

the security evaluation framework (Afolaranmi et al. 2018). To validate the relevance of the CBISEF, the Pearson Product Moment Correlation was used in which the reviewers' rating score for each item in a cluster of aspects of the framework was correlated with the total score of that cluster. Items that significantly correlated with the total score at p-values < 0.05 were regarded as being valid or relevant in the evaluation framework.

### **The relevance of six components in the cloud business intelligence security evaluation framework**

Table 7.1 shows the relevance of each of the six components of the framework based on the Pearson Product Moment Correlation analysis.

**Table 7.1: Relevance of each of the six components of the framework**

| <b>Component of the security framework</b>                             | <b>Overall components rating (n =19)</b> |                        |
|--|--|------------------------|
|  | <b>Pearson Correlation</b>               | <b>Sig. (2-tailed)</b> |
| Alignment of data management and security needs to business objectives | 0.735**                                  | 0.000                  |
| Cloud business intelligence security and usability                     | 0.407**                                  | 0.004                  |
| Cloud business intelligence service delivery models                    | 0.671**                                  | 0.002                  |
| Cloud deployment models  | 0.782**                                  | 0.000                  |
| Cloud service providers  | 0.671**                                  | 0.002                  |
| Financial risks due to security risks                                  | 0.674**                                  | 0.002                  |

\*\* Correlation is significant at the 0.01 level (2-tailed).

The correlation results show that all six components of the CBISEF were significantly correlated to the overall rating of all components at  $p < 0.05$ . This validated the six components of the CBISEF as being relevant in the security evaluation process and therefore, justifies the inclusion of each component in the framework.

Reviewers were asked to assess the relevance of the activities to be performed in each of the six components of the proposed framework during the evaluation process. The results of the Pearson Product Moment Correlation analysis for the validation are shown in *Table AP7.2 in Appendix L*. The Pearson Product Moment Correlation scores of most of the suggested activities correlated



significantly with the overall ratings of the respective clusters at  $p < 0.05$ . This indicated that all activities were validated as being relevant in their respective components of the proposed CBISEF. The three suggested activities that can be performed at the beginning of the evaluation process were relevant, indicated by their strong correlation with the total at  $p < 0.00$ . For the second component, Assessing the security controls in place and their robustness, there was no significant correlation with the overall ratings of the respective cluster at  $p < 0.05$ , unlike the other activities. This indicated that the activity being dealt with was less likely to be relevant in that CBISEF component.

For the assessment of cloud business intelligence service delivery models, all three activities were found to be very relevant as they were strongly correlated to the overall rating of the cluster at  $p < 0.00$ . This confirmed that it was important for these activities to be carried out in this stage of the evaluation.

The six activities suggested for the assessment of cloud deployment models during the evaluation stage were all validated as relevant, correlating significantly with the overall score of the cluster at p-values 0.035 to 0.00. However, the degree of relevance varied, with those activities relating to finance implications ( $r=0.856$ ;  $p < 0.00$ ) gaining more emphasis than the security ones ( $r = 0.485$  at  $p < 0.035$ ). The relevance of knowledge of the deployment model is highlighted by a correlation of 0.815 at  $p < 0.00$ .

Six activities were proposed for the assessment of cloud service providers and were all found very relevant or relevant, as their ratings correlated significantly with the overall score of the component at p-values between 0.013 and 0.00. The correlation scores of 0.557 to 0.849 at  $p < 0.013$  were evident enough that the reviewers viewed the activities as being relevant and should be included in this component. Similarly, financial implications received more relevance than other activities.

Finally, the four activities in assessing financial risk in cloud business intelligence were rated as very relevant with very high correlations scores of 0.712 to 0.902 at p-values of 0.001. These results indicated that the financial issues of the enterprises were essential, and the evaluation process should cater for these issues.

Two more important validations for the CBISEF were done to check the inclusion of ideas from other frameworks and standards and the overall relevance of the framework. Results in Table 7.3 show the correlation results.

**Table 7.2: Validating framework concerning traditional frameworks**  
(n = 19)

| Validation aspect and criteria   | Overall cluster rating |                 |
|--|------------------------|-----------------|
|  | Pearson Correlation    | Sig. (2-tailed) |
| <b>The relevance of security evaluation in addressing standard frameworks</b>                          |                        |                 |
| COBIT for IT governance and bringing in the best practices   | 0.734**                | 0.000           |
| ISRM for assessing security risks in assets and managing them  | 0.877**                | 0.000           |
| ISO 2701 for compliance to standards for information security policies and standards and certification | 0.807**                | 0.000           |
| NIST for cybersecurity assessment and management   | 0.899**                | 0.000           |
| ERM for Cloud Computing to assess cloud environments   | 0.800**                | 0.000           |
| <b>Overall rating of the relevance of the framework in</b>   |                        |                 |
| Addressing cloud business evaluation challenges faced by SMEs  | 0.557*                 | 0.013           |
| Addressing various conventional security frameworks  | 0.910**                | 0.000           |
| Aiding SMEs in evaluating cloud business intelligence and other cloud services                         | 0.892**                | 0.000           |

\* Correlation is significant at the 0.05 level (2-tailed). \*\* Correlation is significant at the 0.00 level (2-tailed).

The activities suggested in the six components were validated for addressing issues similar to the convention framework and standards such as the COBIT, ISRM, ISO2701, NIST, and ERM. The Pearson Correlation scores of the five aspects ( $r = 0.734$  to  $0.899$ ) indicated a significant strong association with overall cluster ratings at p-values between 0.000 and 0.013. This further confirmed that the activities in all six components were included on the strengths of the fact that they addressed important issues in the conventional frameworks and standards.

Overall, the CBISEF was validated as relevant in addressing the evaluation challenges faced by SMEs ( $r = 0.557$ ;  $p < 0.013$ ), which the conventional security framework addressed ( $r = 0.910$ ;  $p = 0.00$ ). The validation process confirmed that the CBISEF could aid SMEs in evaluating Cloud BI and other cloud services ( $r = 0.892$ ;  $p = .000$ ).

### Overall relevance validation of the framework

For the overall validation, the overall score for the six components and overall scores for the activities were tested against the overall rating score for 39 constructs, used in relevance validity, as rated by 19 reviewers. The Correlation Coefficient shows a significant association among variables tested, suggesting that the reviewers were validating that the components of the CBISEF, the checklists and the activities, which should be conducted during the evaluation process, were relevant. The results are depicted in Table 7.3.

**Table 7.3: Validation of overall relevance of aspects of the framework**

**n = 19**

| Validation of overall relevance of aspects of the framework  | Overall relevance   |                 |
|--|---------------------|-----------------|
|  | Pearson Correlation | Sig. (2-tailed) |
| The relevance of the component of the security framework   | 0.839**             | 0.000           |
| Relevance in assessing the alignment of data management and security needs to business objectives            | 0.720**             | 0.001           |
| Relevance in assessing cloud business intelligence security and usability                                    | 0.867**             | 0.000           |
| Relevance in assessing cloud business intelligence service delivery models                                   | 0.845**             | 0.000           |
| Relevance in assessing cloud deployment models   | 0.824**             | 0.000           |
| Relevance in assessing cloud service providers   | 0.920**             | 0.000           |
| Relevance in assessing financial risks due to security risks   | 0.848**             | 0.000           |
| The relevance of framework in addressing traditional security standards and frameworks during the evaluation | 0.509*              | 0.026           |
| Overall rating of the relevance of the framework   | 0.839**             | 0.000           |

\* Correlation is significant at the 0.05 level (2-tailed). \*\* Correlation is significant at the 0.01 level (2-tailed).

The results show a significant association between the overall relevance of components and suggested activities of the CBISEF framework and the overall score of measured aspects at  $p < 0.05$ . These results show that the proposed components and activities of the formulated framework were relevant in Cloud BI evaluation by non-IT security specialists. Although the results showed that all validated aspects were relevant to the security evaluation process, differences in Pearson Correlations showed some variations in the appropriateness of the activities to be conducted in each component. Assessing cloud service providers were found to be highly relevant,  $r = 0.920$  at  $p = 0.000$ , while the relevance of the framework in addressing traditional frameworks and the standard was least relevant  $r = 0.509$  at  $p = 0.026$ . These results confirm that the CBISEF could

adequately address security evaluation challenges by SMEs where there are non-IT security specialists.

#### 7.4.2. Acceptance validation using face validity analysis

The results for this validation were presented as descriptive and inferential statistics.

##### i. Acceptance validation results in descriptive statistics

This validation was intended to determine whether the CBISEF components, activities, and checklists were acceptable by intended users and IT security specialists in cloud security. Data were collected employing an online closed-ended questionnaire from a sample of 10 IT security specialists and 24 SME decision-makers. Table 7.4 shows the demographic characteristics of CBISEF acceptance reviewers.

**Table 7.4: Demographic information of acceptance reviewers**

(n = 34)

| Demographic characteristic        | F  | %    |
|-----------------------------------|----|------|
| <b>Gender of reviewers</b>        |    |      |
| Female                            | 13 | 38.2 |
| Male                              | 21 | 61.8 |
| Total                             | 34 | 100  |
| <b>The age range of reviewers</b> |    |      |
| 20 to 30                          | 15 | 44.1 |
| 31 to 40                          | 6  | 17.6 |
| 41 to 50                          | 12 | 35.3 |
| above 50                          | 1  | 2.9  |
| Total                             | 34 | 100  |

Of the 34 reviewers, 13 were females and 21 were males. Most of the reviewers were aged between 20 and 50. Results in Table 7.5 show that 24 (70.6%) were decision-makers and 10 (29.4%) IT security specialists.

The educational background of the reviewers was an important demographic characteristic used in this study. Results in Table 7.5 depict the educational status of the reviewers used. A cross-

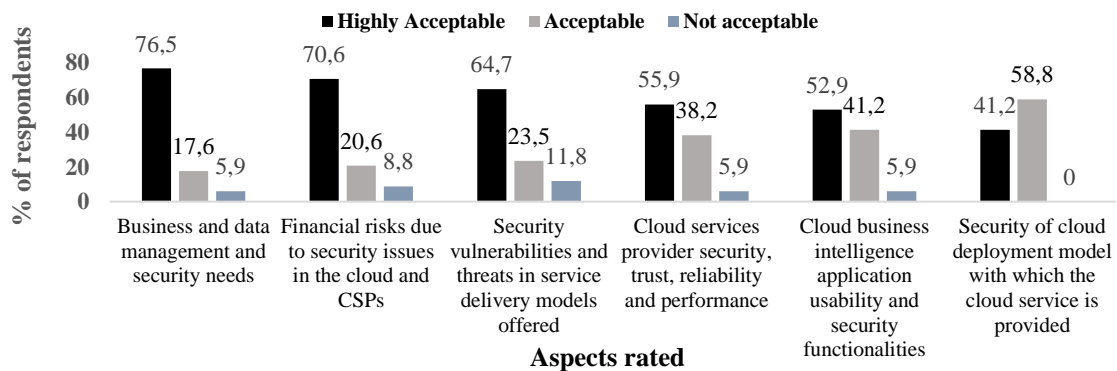
tabulation of occupation and educational qualifications indicates that 11 (32.3%) decision-makers had diplomas and 13 (38.2%) degrees. Comparatively, 8 (23.5%) of the IT security specialists held various degrees. The results show that the reviewers had a good educational background which was important in the validation of the framework.

**Table 7.5: Educational background of reviewers**

| Educational Qualification (n = 34) |         |      |        |      |       |      |
|------------------------------------|---------|------|--------|------|-------|------|
| Occupation of reviewer             | Diploma |      | Degree |      | Total |      |
|                                    | n       | %    | n      | %    | n     | %    |
| Decision-makers                    | 11      | 32.3 | 13     | 38.2 | 24    | 70.6 |
| IT Security specialists            | 2       | 5.9  | 8      | 23.5 | 10    | 29.4 |
| Total                              | 13      | 38   | 21     | 62   | 34    | 100  |

Face validation of the framework involved reviewing six components, the activities, and the checklists for their acceptability by the intended users, the SME decision-makers. The reviewers were asked to study the framework, activities and checklist and rate the acceptability of each on a 3-point Likert scale (highly acceptable = 3; acceptable = 2 and not acceptable = 1). The reliability of the 30 items measured by Cronbach's Alpha was 0.946, indicating a strong consistency in the instrument used for face validity. Figures 7.1 to 7.7 depict the results of the acceptability of various aspects of the CBISEF by reviewers.

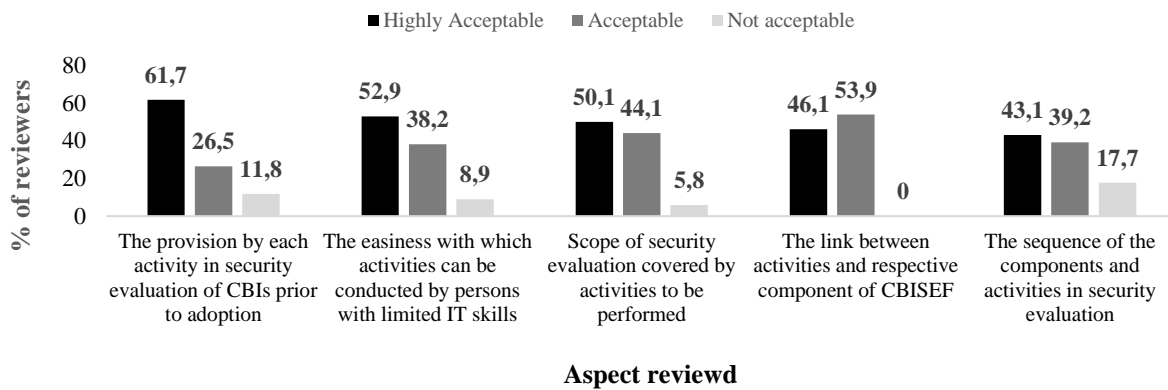
Figure 7.1 shows the ratings on the acceptability of each component of CBISEF for us by SMEs



**Figure 7.1: Ratings of the acceptability of each component of CBISEF by SMEs**

The results show that five components of the CBISEF were rated as highly acceptable by at least 53% of the reviewers and one as acceptable by 58% of the reviewers. This confirms that all the components were validated as being acceptable for being part of the CBISEF and appropriate for use by non-IT Security specialist decision-makers in SMEs.

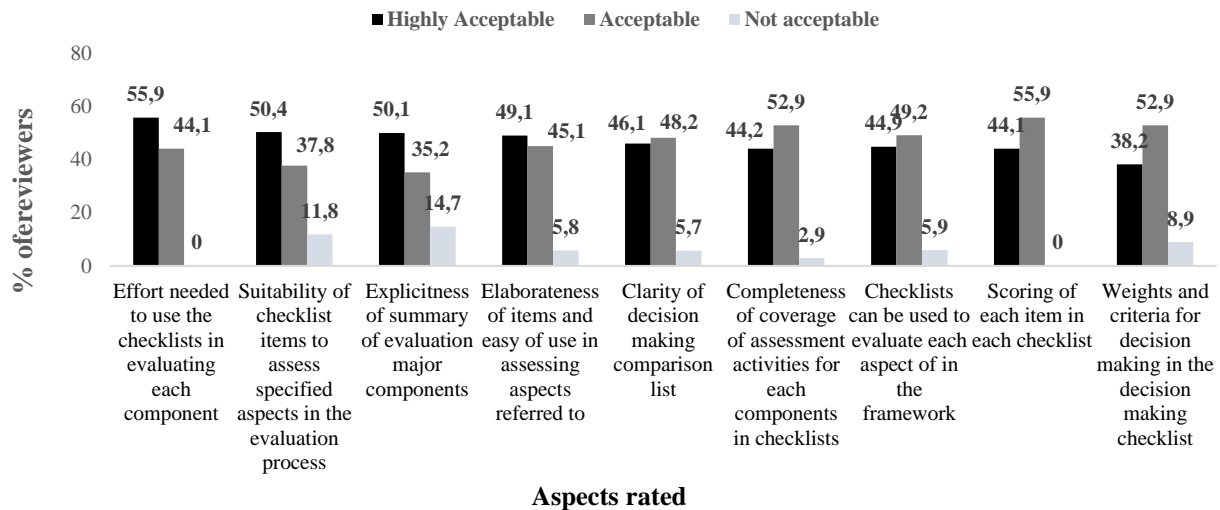
Figure 7.2 shows the results of the review for the acceptability of the activities on the checklists that were supposed to be performed during the evaluation process.



**Figure 7.2: Ratings of acceptability of Cloud BI security evaluation activities in checklists**

The results were arranged according to the level of acceptability of the activities. Most of the reviewers, 61.7%, confirmed that suggested activities in the security evaluation of Cloud BI before the adoption were highly acceptable. The ease with which activities can be performed by non-IT personnel was rated highly acceptable by 52.9% and acceptably by 38.2% of the reviewers. Most of the reviewers, 50.1% rated the scope of security evaluation covered by activities highly acceptable, while 44.1% rated it acceptable. The link between activities and respective components of CBISEF was rated by 46.1% highly acceptable and by 53.9% as acceptable. The sequence of components and activities in security evaluation was rated by 53.1% highly acceptable and 39.2% acceptable. In all cases, the minority of the reviewers expressed the unacceptability of each criterion reviewed, with the sequence of the components and activities in security evaluation having 17.7%, refuting the acceptability of this checklist activity. Overall, the majority of the reviewers indicated high acceptability of the checklists and the suggested activities.

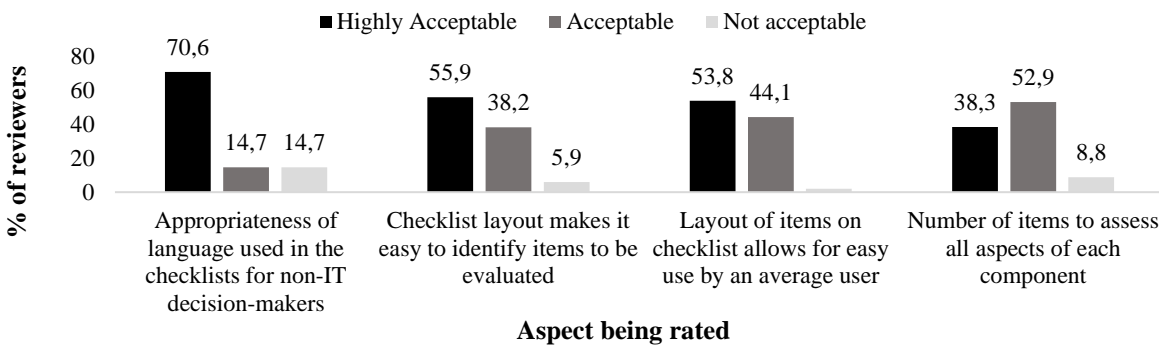
The acceptability of the checklists was validated using the 3-point-Likert-type scale alluded to above. The review focused on the user’s effort using checklists, the suitability of items, the explicitness of items, item elaborateness, clarity and completeness, suitability, scoring, and weighting used. The results are depicted in Figure 7.3 showing the acceptability ratings of the checklist aspects. The results show that the checklists were acceptable in all nine aspects which were reviewed. Acceptability ratings for the effort needed to use the checklists, the suitability of the checklist, and explicitness were highly acceptable as indicated by most of the respondents (50 to 60%). This shows that reviewers accepted the checklist based on ease of use, clarity of what was to be evaluated and how the evaluation should be conducted. The scoring system used in the checklists was highly acceptable as it consisted of basic metric systems that are understood by basic IT users. A minor difference of less than 11% between highly acceptable and acceptable ratings was observed for the elaborateness, clarity, completeness, appropriateness of the checklist, scoring, and weighting of each criterion used. The results show that the nature of the checklists was validated as acceptable regarding the components of the CBISEF and the level of knowledge of decision-makers who would use these tools.



**Figure 7.3: Rating of acceptability of checklists aspects**

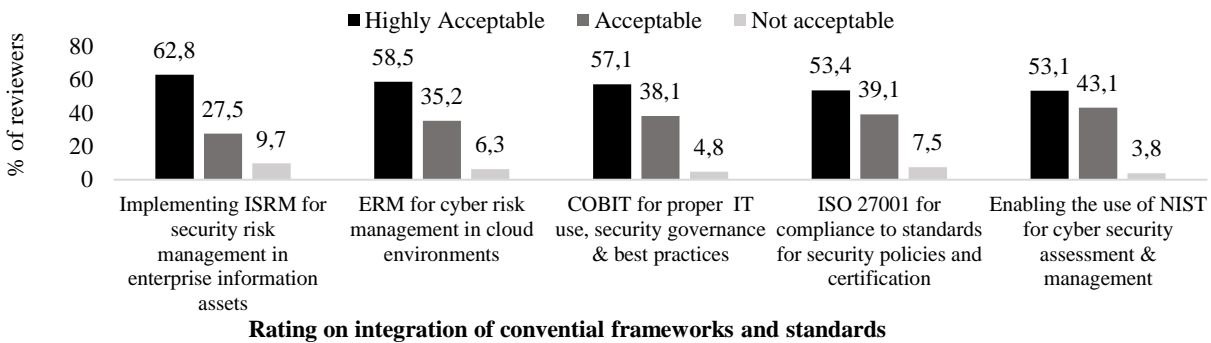
The validation was extended to the language used in the checklists, the number of activities to be done, the layout of activities and ease of use. The results in Figure 7.4 show that these items were either highly acceptable or just acceptable. Most of the reviewers, 70.6%, indicated that the

language used was highly acceptable for the framework of this type. The layout of the checklist was highly acceptable for 55.9% of reviewers and ease of use due to the layout was highly acceptable for 53.8%, while 44.1% of reviewers indicated the checklists were acceptable. For the number of activities to be conducted per component, 39.3% confirmed it to be highly acceptable, while the majority, 52.9%, rated these as acceptable. It could be inferred from these results that the checklists were acceptable for use by SMEs with regards to the language used, the layout of the items, their easy location, and the appropriate number of items involved.



**Figure 7.4: Acceptability of language used, length and layout of checklists**

The integration of conventional security frameworks and standards into the CBISEF was another important validation criterion used in this study. Reviewers were asked to rate the integration of five selected conventional security frameworks and standards in the CBISEF. Figure 7.5 depicts the results.

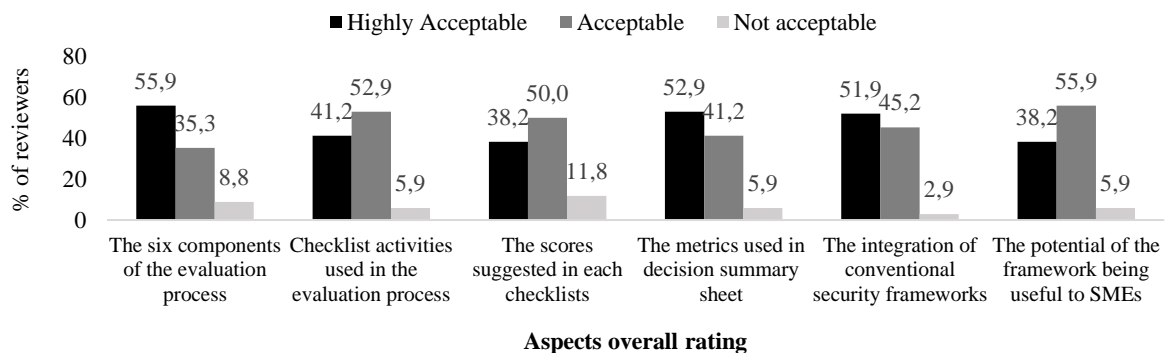


**Figure 7.5: Acceptability of the proposed framework in implementing traditional security standards and frameworks**



At the basic level of security evaluation in Cloud BI, the majority of reviewers (90% and above) rated the integration of the selected security framework and standards as being acceptable and highly acceptable. At least 50% of the reviewers indicated that they would accept the CBISEF for addressing basic security requirements based on the existing security frameworks and standards. The integration of ISRM and ERM were rated highly acceptable as these were the basic requirements for IT and cloud security that SMEs were supposed to consider at the initial evaluation of Cloud BI. The inclusion of evaluation activities that enabled the integration of COBIT for proper IT use and security, governance and best practices was another important aspect that reinforced the acceptability of the CBISEF and checklists by 57.1% of the reviewers. ISO 27001, which enabled SMEs to evaluate compliance to standards for security policies and certification was vital to the validation of the CBISEF and the checklists positively contributed to the high acceptability of the framework. This was needed to enable SMEs to check the security compliance of the Cloud BI and providers. The results show that the reviewers accept the CBISEF for its potential to enable decision-makers to use selected aspects of NIST for cybersecurity assessment and management. These findings show that the CBISEF fuses important aspects of the existing framework on the best practices of SMEs in their quest to adopt and use Cloud BI.

The overall review of CBISEF acceptability was based on the six components, checklist activities, scores, basic metrics, integration of conventional security frameworks, and the potential to be used by SME decision-makers. The results are shown in Figure 7.6.

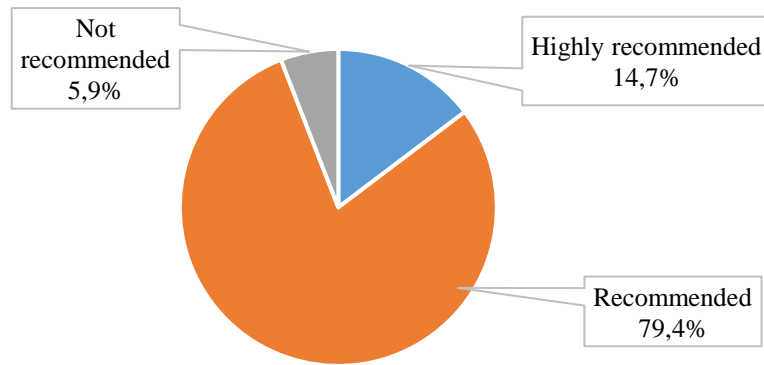


**Figure 7.6: Overall rating of the acceptability of each aspect of the framework**

The overall validation results show that all six aspects reviewed, validated the CBISEF as generally acceptable as shown by the majority of reviewers' high ratings of highly acceptable and acceptable. Most importantly, the six components of the CBISEF were rated as highly acceptable by close to

56% of the reviewers. The potential of the framework being useful to SMEs was rated acceptable by close to 56% of the reviewers. Based on these results, it could be deduced that the proposed CBISEF was validated as being overall acceptable, in components, checklists, activities subjected, basic metrics, addressing standards and certifications, and its usefulness to SMEs in selected towns.

Finally, reviewers were asked to indicate how they would recommend the acceptability of the Cloud BI framework, using a 3-point Likert scale (Highly recommended = 3, Recommended = 2, and Not recommended = 1). The results of the recommendations are depicted in Figure 7.7.



**Figure 7.7: Overall recommendation for acceptability**

The results show that most of the reviewers, 79.4%, indicated that they would recommend the CBISEF as an acceptable framework suitable for the purpose for which it was designed.

**i. Inferential statistics**

Chi-square tests were conducted to examine the relationship between the acceptability of the CBISEF for (a) the six components; (b) suitability of activities on the checklists; (c) checklist scores; (d) the metrics used in the decision summary sheet; (e) the integration of various conventional security framework; (f) the potential of the framework to be useful to SMEs; (g) recommendation for acceptability; and (h) the type of the reviewers. The results are shown in Tables 7.6 and 7.7. There is a significant relationship between the type of reviewers and the overall acceptability of the proposed components of the CBISEF. It shows that 70% of IT security specialists and 62.5% of respondents were more likely to rate the six components as highly

acceptable than SME managers,  $X^2(1, N = 34) = 11.04, p < 0.026$ . This further validates the six components as acceptable to be in the proposed framework.

**Table 7.6: Chi-square test for framework components acceptability on reviewers**

| Type of reviewer        | Details   | Acceptability of the six components in the evaluation process |            |                | Total  |
|-------------------------|---|---|------------|----------------|--------|
|                         |   | Highly acceptable   | Acceptable | Not acceptable |        |
| SME managers            | Count   | 1   | 5          | 2              | 8      |
|                         | % within Type of reviewer                             | 12.5%   | 62.5%      | 25.0%          | 100.0% |
|                         | % within The six components of the evaluation process | 5.6%  | 35.7%      | 100.0%         | 23.5%  |
| SMEs owners             | Count   | 10  | 6          | 0              | 16     |
|                         | % within Type of reviewer                             | 62.5%   | 37.5%      | 0.0%           | 100.0% |
|                         | % within The six components of the evaluation process | 55.6%   | 42.9%      | 0.0%           | 47.1%  |
| IT Security specialists | Count   | 7   | 3          | 0              | 10     |
|                         | % within Type of reviewer                             | 70.0%   | 30.0%      | 0.0%           | 100.0% |
|                         | % within The six components of the evaluation process | 38.9%   | 21.4%      | 0.0%           | 29.4%  |
| Total                   | Count   | 18  | 14         | 2              | 34     |
|                         | % within Type of reviewer                             | 52.9%   | 41.2%      | 5.9%           | 100.0% |
|                         | % within The six components of the evaluation process | 100.0%  | 100.0%     | 100.0%         | 100.0% |

**Chi-Square Tests**

|                    | Value               | df | Asymptotic Significance (2-sided) |
|--------------------|---------------------|----|-----------------------------------|
| Pearson Chi-Square | 11.037 <sup>a</sup> | 4  | 0.026                             |
| Likelihood Ratio   | 11.282              | 4  | 0.024                             |
| N of Valid Cases   | 34                  |    |                                   |

a. 6 cells (66.7%) have an expected count of less than 5. The minimum expected count is 34.

Moreover, the above Chi-square test results for the other six aspects in Table 7.7, show that acceptability was independent of the types of reviewers involved in the study, as shown by  $p > 0.05$ . This further confirmed that the CBISEF was validated as acceptable by the three types of reviewers based on the appropriateness of the components, checklists and basic metrics used in the evaluation.

**Table 7.7: Chi-square tests of independence based on the type of reviewers**  
(n=34)

| <b>Overall acceptability tested</b>                        | <b>Pearson Chi-Square</b> | <b>df</b> | <b>Asymptotic Significance (2-sided)</b> |
|--|---------------------------|-----------|--|
| The suggested evaluation activities in the checklists      | 5.505                     | 4         | 0.239                                    |
| The checklists scores suggested in each checklist          | 4.223                     | 2         | 0.121                                    |
| The metrics used in the decision summary sheet             | 7.215                     | 4         | 0.125                                    |
| The integration of various conventional security framework | 4.187                     | 2         | 0.123                                    |
| The potential of the framework is useful to SMEs           | 5.962                     | 2         | 0.061                                    |
| Recommendation for acceptability                           | 0.914                     | 2         | 0.633                                    |

#### **7.4.2.1. Suggestions and modifications**

IT security specialist reviewers suggested the reduction in the number of checklists by removing the Summaries of assessment of evaluation criteria, which they thought was a duplication of the Summary of evaluation of major components of framework decisions. Furthermore, the reviewers recommended the removal of sub-totals from other checklists as well as reducing the number of activities to be conducted. The suggestions were implemented in the final checklists.

### **7.5. Discussions**

The proposal of the framework has been justified by both literature and empirical studies conducted in previous chapters. Framework validation was the ultimate stage in the development of the framework as it provided the researcher with an opportunity to have input from IT security specialists to improve the product before its adoption and use by the intended users. The proposed CBISEF was validated for relevance to the purpose for which it was designed and overall acceptability for use by the intended enterprises. Information Security Forum (2016) emphasises the importance of involving affected enterprises if one is to develop a relevant and acceptable solution. From the validation results, the CBISEF is suitable for POUE in SMEs where there are no IT specialists. Studies on framework and model validation highlight various techniques that the researcher can use and the inherent challenges (Yusoff 2019; de Jongh et al. 2017; Mussa et al. 2016). These studies encourage the use of non-mathematical validation techniques that enable other users who are interested in the validation to be able to evaluate the framework before adoption (Yusoff 2019; de Jongh et al. 2017). The validation techniques used in this study were

meant to be inclusive and as simple as possible for use by non-IT specialists to be able to inspect and even use the framework to assess Cloud BI of their own choice.

The results of the validation process show that reviewers were satisfied with the relevance of the aspects covered for each component, which included basic information on security risk management requirements as specified in the ISRM, COBIT and NIST cybersecurity (Mirai Security 2019). The framework gives the SMEs a leeway to systematically evaluate Cloud BI before the adoption, using a system of checklists at various stages of the evaluation process, a recommendation by Cloud Security Alliance (2017) and Mirai Security Inc (2019). Scores used in the checklists can enable the users to be objective when inspecting various security aspects of the Cloud BI in each component. By using the checklists, there is no doubt that users will be able to ascertain that the Cloud BI meet certain criteria as a security requirement to be considered for the next step in the evaluation. According to Yusoff (2019), manually validated tools enable the reviewers to identify flaws that may not be possible with computerised systems. The correlation results indicated strong positive associations between overall relevance and the components of the framework at  $p < 0.05$ . This validated that the CBISEF consisted of the relevant aspects suggested by SME decision-makers during the interview and quantitative survey. Therefore, the components were closer to what SMEs in the selected towns of the Limpopo Province envisaged to be suitable for their purpose. This was supported by IT security specialists and IT specialists who participated in this study. The Chi-square test confirmed that the acceptability validation was independent of the types of reviewers involved,  $p > 0.05$ . The content validity confirmed the relevance of the framework and the face validity confirmed the acceptability of the CBISEF framework for use by SMEs in the selected towns in Limpopo Province.

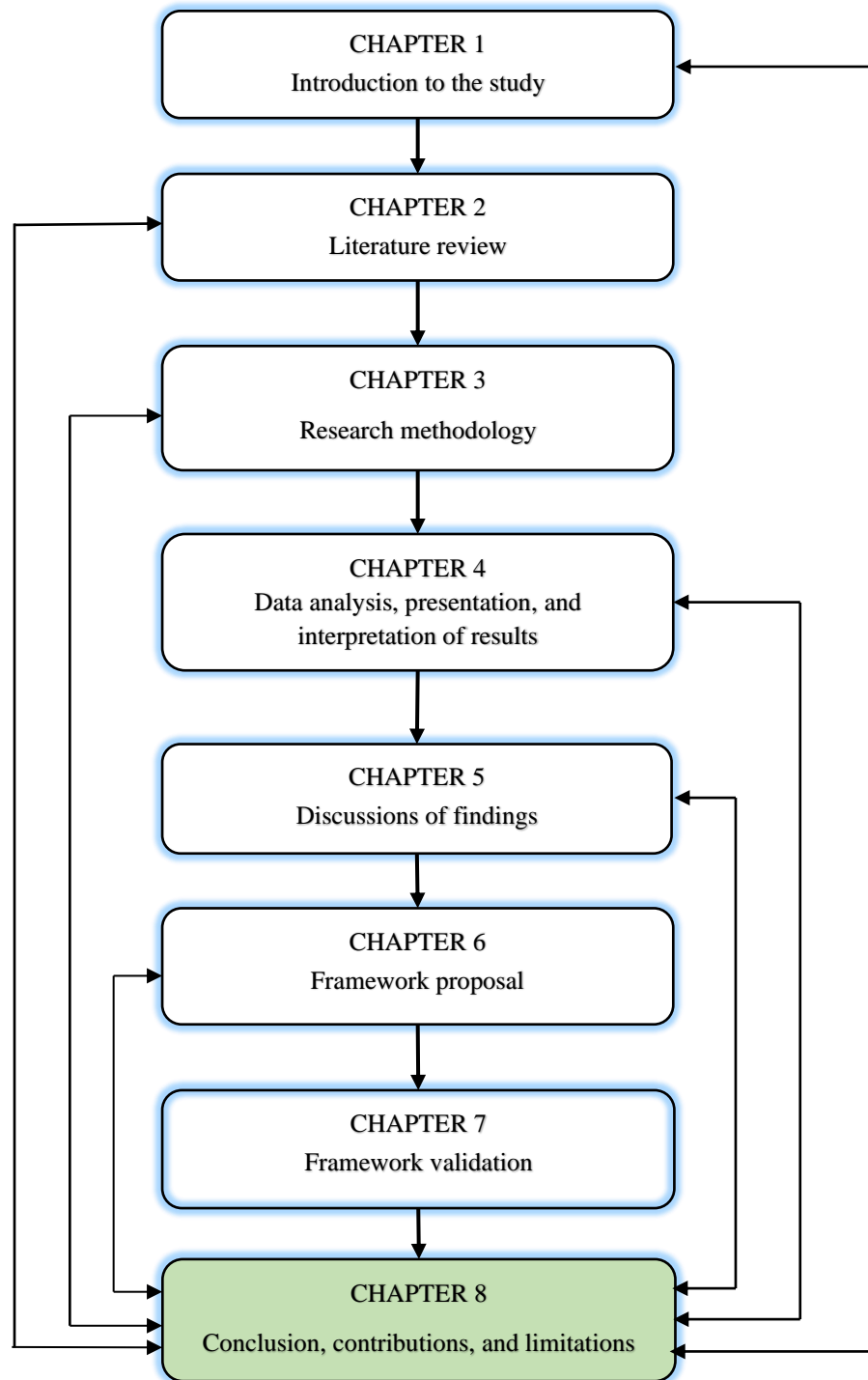
## **7.6. Conclusion**

This chapter dealt with the validation for relevance and acceptance of the CBISEF using empirical data from two samples of reviewers, namely IT security specialists, IT specialist and SME decision-makers. The validation was conducted using correlations for relevance, descriptive statistics and Chi-square tests for acceptability. The six components of the CBISEF, checklists, activities, scores, metrics, and integration of conventional security frameworks were found to be relevant with correlations at  $p < 0.05$ . The descriptive statistic results revealed that both IT

specialists and SME reviewers rated the CBISEF as acceptable in all aspects reviewed. This was confirmed by the Chi-square test, which showed the acceptability of the CBISEF independent of the type of reviewers. The reviewers recommended reducing the number of summary worksheets by removing the Summary activity evaluation worksheet which was a duplicate of the Summary evaluation sheet. Overall, the findings validated the relevance and acceptance of the CBISEF as an appropriate and suitable framework, whose components, checklists, and metrics were expected by SMEs in targeted towns in the Limpopo Province.

The next chapter evaluates and synthesises the study as conclusions, the contribution of the study to the existing body of knowledge, limitations to the study and further research emanating from the study.

## CHAPTER 8 CONCLUSIONS, CONTRIBUTIONS AND LIMITATIONS OF THE STUDY



## 8.1. Introduction

The foregoing chapter discussed the validation of the proposed framework in terms of relevance by IT specialists and acceptability by SME decision-makers in the five selected towns of the Limpopo Province. The purpose of this chapter is to provide an overview of the study, conclusions, contribution to the existing body of knowledge, limitations of the study, and a recommendation for future research.

## 8.2. Summary of the study

The purpose of the study was to propose an easy-to-use security evaluation framework for Cloud BI, suitable for use by SMEs in disadvantaged small South African towns with scarce IT specialists. Selected towns in the Limpopo Province were used as study units. This thesis consists of eight chapters, each dealing with an important aspect of the study.

Chapter 1 introduced the research study by providing an insight into the problem being solved and the extent to which it affected the SMEs in the Limpopo Province when adopting Cloud BI. The major objective of the studies was: *To propose a security evaluation framework for Cloud BI for use by SMEs in under-resourced small towns in the Limpopo province.* The study was designed to answer the main research question: *What are the main components of a security evaluation framework for Cloud BI suitable for small and medium enterprises in under-resourced small towns in the Limpopo province?* Table 8.1 presents the four minor objectives that were achieved and the four sub-research questions that were answered. The research questions were explored from both theoretical and practical perspectives. Theoretical perspectives involved conducting a literature review from scholarly sources, databases, and reports from security and government institutions. The literature review was presented in Chapter 2. The literature reviewed revealed that several initiatives in place for cloud services adoption did not adequately address the security evaluation of Cloud BI by SMEs. The practical perspective entailed a systematic data collection and analysis, presentation and discussion of results. Chapter 3 provided a detailed account of the methodology used in this study. The research methodology implemented in this study was guided by the Research Onion model in which the exploratory sequential mixed-method design was employed. Data was collected using the interview method in the QUAL phase and the questionnaire method in the QUAN phase. Thematic data analysis was applied to qualitative data, findings were then



presented as themes and sub-themes. Quantitative results were obtained from the analysis of quantitative data using SPSS version 26. An integrated interpretation of findings of the QUAL phase, substantiated by the results of the QUAN phase, was presented in Chapter 4, based on SRQs 1 to 4. Extracts from the interviews were used to support the interpretations. A detailed literature-controlled discussion of the findings was conducted in Chapter 5. In Chapter 6, a six-components security evaluation framework was proposed from the findings made in Chapter 5. A detailed description of each component of the framework was accompanied by a checklist was provided for use by SME decision-makers. Chapter 7 presented a detailed report on the validation of the CBISEF and checklists.

**Table 8.1: List of research objectives and questions**

| Sub-research objectives (SROs)   | Sub research questions (SRQs)   |
|--|---|
| <b>SRO1:</b> To explore factors influencing the adoption and use of Cloud BI by SMEs in small South African towns  | <b>SRQ1:</b> What factors influenced the adoption and use of Cloud BI among SMEs in small towns in Limpopo Province?                                    |
| <b>SRO2:</b> To examine the strategies used by SME decision-makers when evaluating Cloud BI they have adopted or intend to adopt   | <b>SRQ2:</b> How did small and medium enterprise decision-makers evaluate Cloud BI before adoption?   |
| <b>SRO3:</b> To evaluate the critical security evaluation challenges that prevent the adoption of Cloud BI by SMEs   | <b>SRQ3:</b> What challenges did small and medium enterprise decision-makers face when evaluating Cloud BI?   |
| <b>SRO4:</b> To determine what the main components of the security evaluation framework of a Cloud BI were so that it can be used by decision-makers who were not IT specialists | <b>SRQ4:</b> What did decision-makers consider as the main components of a security evaluation framework for Cloud BI for small and medium enterprises? |

### **8.3. Conclusions of the study**

The conclusions for this study are presented for each sub-research question and, then the main question.

#### **8.3.1. Factors influencing the adoption and use of Cloud BI among SMEs in the Limpopo Province**

The study found that the adoption and use of Cloud BI by SMEs were enabled by factors such as: improving decision making, reducing overhead costs by using Cloud BI instead of on-premise BI applications, improving enterprise competitiveness, affordability of cloud services, data analysis, visualisation, and reporting, improving customer care, improving data management, and

enhancing professionalism in information analysis. On the other hand, factors preventing the adoption of Cloud BI by SMEs were fear of data security breaches in the cloud, limited knowledge of how Cloud BI worked, limited security knowledge of Cloud BI, lack of knowledge on which Cloud BI was secure, and mistrust of CSPs. Fear of financial risks was the most deterring factor, preventing the adoption and use of cloud technologies. These findings show that more factors prevented the adoption and use of Cloud BI than enabled it.

The study concluded that the high level of awareness of the benefits of using Cloud BI and the willingness of SME decision-makers to use these applications were poorly sustained due to limited knowledge and the lack of user-friendly security evaluation methodologies and frameworks for use by non-IT specialists. Factors preventing the adoption of Cloud BI were more influential on decision-makers than enabling ones. Fear of financial risks due to the use of Cloud BI without proper security evaluation was the overall influential factor that decision-makers suggested should be addressed by a security evaluation framework suitable for SMEs. The impact of the deterring factors outweighed the benefits of using Cloud BI thereby reducing the eagerness of decision-makers to adopt the technology. Although decision-makers knew about Cloud BI, they did not have much knowledge of how secure the applications were, therefore they opted to evaluate or delay adoption.

### **8.3.2. Strategies used by SME decision-makers to evaluate Cloud BI before adoption**

Despite the low level of adoption of Cloud BI by SMEs, the study concluded that decision-makers were making efforts to assess various Cloud BI and other cloud services. The strategies employed in the evaluation were not systematic as these were ad hoc because individual enterprises relied much on information sourced from friends and the open web. The actions taken by each SME during the evaluation process was not documented. SME decision-makers were not familiar with industry security frameworks and standards; therefore, the evaluation process did not apply any best practices. The knowledge of security evaluation among decision-makers was limited to the basic activities they regarded as important, and some were indirectly linked to the best practices of the industry, standards, and procedures. Overall, decision-makers appreciate the value of security evaluation when selecting Cloud BI before they make the final selection.

### **8.3.3. Challenges faced by SME decision-makers when evaluating Cloud BI**

The study concluded that limited knowledge of Cloud BI and lack of user-friendly security evaluation tools were the major challenges among SME decision-makers who considered adopting and using the technology. Decision-makers resorted to unorthodox evaluation strategies because they perceived industry standards and frameworks as too complicated to use and that they do not address the problems faced by SMEs during the adoption process.

### **8.3.4. Main considerations made when evaluating Cloud BI**

Although decision-makers lacked the technical knowledge and skills to evaluate Cloud BI, they had expectations of what should be considered during the evaluation process. The considerations were grouped into five categories from which the components of the security evaluation framework were proposed. Based on these categories, the study concluded that the main components of the security evaluation framework should address six major areas which were of concern to decision-makers, namely enterprise data security; security vulnerabilities; threats, security, trust and performance of CSPs; and risks of Cloud BI; security in cloud deployment models; security of service delivery models; and financial risks due to various security issues and litigation. The major concern of SMEs were financial risks resulting from loss of business competitiveness. These major considerations were blended with best practices from the existing industrial framework and standards for easy implementation by non-IT SME decision-makers. Decision-makers tend to be influenced by what they can benefit from the use of cloud services, the security risks the business is likely to be exposed and the ease with which the cloud is used (Salim et al. 2014). These are the tenants of TPB, TAM and DoIT (Salim et al. 2015; Evens et al. 2008; Sahin 2006; Ettlie 1980).

### **8.3.5. The main components of a security evaluation framework for Cloud BI for SMEs**

The main components of the security evaluation framework for Cloud BI consist of six major aspects, each with activities to be assessed during the evaluation process, using user-friendly checklists. However, financial risks are central and should be addressed at each stage of the evaluation process. The framework and its six checklists were validated as relevant by IT security specialists and acceptable by intended users, namely the SME decision-makers. Correlation analysis showed a significant association between individual components with the overall

relevance of the framework at  $p < 0.05$ , leading to the conclusion that IT-security specialists regarded the components as covering the important aspects to be evaluated. Chi-square test analysis showed a significant association between the acceptability of individual components and the overall framework at  $p < 0.05$ , indicating that users accepted the framework components and checklist activities as being important in the evaluation process. Based on the validation results, the study concluded that the CBISEF and the six checklists were relevant and acceptable as a solution to the existing problems faced by SMEs in the evaluation of Cloud BI by non-IT specialists based in under-resourced towns in the Limpopo Province.

#### **8.4. Contribution to the existing body of knowledge**

The scope of this study was limited to the security evaluation of Cloud BI before adoption among SMEs in disadvantaged small towns in the Limpopo Province. The main contribution of this study was the proposed security evaluation framework for Cloud BI suitable for use by SME decision-makers who are non-IT specialists. According to Agerfalk (2010) and Scott (2016), a model, a methodology, or a framework is a form of functional knowledge needed to bring about action within selected entities within business societies. The framework produced in this study is a scientific contribution to functional knowledge in IS research and is important in providing SMEs with guidance in their efforts to select the most appropriate Cloud BI solutions for their businesses. The study contributed to the knowledge needed for interventions in the real world to implement different security evaluation strategies and tactics that can benefit SMEs in the use of emerging technologies (Kelly & Cordeiro 2020; Farjoun et al. 2015; Morgan 2014b; Goldkuhl 2012).

The proposed security evaluation framework has practical applications in solving problems faced by SMEs when selecting Cloud BI. This implies that the framework has business value in facilitating SMEs to select the most appropriate Cloud BI to aid effective and timely business decision-making to improve operations and subsequently, viability and competitiveness.

Furthermore, this study contributed to the existing knowledge, in the form of literature, on Cloud BI adoption in disadvantaged small towns in Limpopo. This has been a grey area and peripheral in information systems research in South Africa. Additionally, the study identified the main challenges SMEs faced when evaluating Cloud BI, which were overlooked by previous studies on

cloud services adoption and use. SMEs have different technology needs from LBEs and use different strategies for assessing security in technology, a task done by decision-makers.

From the pragmatic epistemological perspective, this study contributed to three forms of knowledge, namely prescriptive, revealing, and innovative, which are all knowledge for action needed by SMEs to bring about change in their organisations using best practices when adopting cloud technologies. The framework and the checklists lend themselves to prescriptive knowledge and require SMEs to implement them and acquire knowledge and skills in systematically evaluating Cloud BI. The study has shown that the CBISEF was a result of a thorough analysis of data on the practices of SMEs when adopting and using cloud services, particularly Cloud BI. Therefore, revealing knowledge was observed from what has been taken for granted about the needs of SMEs when adopting cloud services. This study was the first of its type in the Limpopo Province and has brought to light what SMEs were doing when attempting to adopt cloud technology. The proposed CBISEF contributes to knowledge for action as it provides enterprises with an alternative systematic means of solving the challenges in security evaluation in Cloud BI.

The academic contribution of the study narrowed the knowledge gap in the security evaluation of Cloud BI by SMEs, which was not addressed in previous studies on the adoption of cloud services. Unlike in previous studies, this thesis identified the challenges faced by SMEs in the adoption of Cloud BI and then provided a scientific solution that was validated by IT-security specialists as relevant for the purpose it was developed. The study provided methodical literature on how pragmatism and mixed methods could be used to solve real-world problems faced by SMEs in disadvantaged communities. Chapters 6 and 7 provide the literature on framework formulation and validation, which provides insights into Cloud BI evaluation using the CBISEF and checklists. The security evaluation framework is flexible and supported by checklists that are for easy use by decision-makers to adapt to the needs of individual SMEs without much assistance from IT security specialists.

### **8.5. Limitations of the study**

This study had several shortcomings beyond the control of the researcher, and these could have affected the outcome of the research. The limitations were due to the newness of Cloud BI among

SMEs, the phenomenon being studied, the location where the study was conducted, access to the participants, the sample size for the QUAN phase, the sampling methods, selection of data and the scope of the characteristics of the technology. The newness of Cloud BI among SMEs in small towns of Limpopo had a direct effect on sample sizes used as there were very few enterprises using the technology. Furthermore, the phenomenon of security evaluation was unfamiliar among SMEs, further reducing the participating enterprises. The SMEs involved in this study were drawn from different economic activities and this could have affected their use of IT systems and cloud services, hence the understanding and requirements of security in their systems. The quality of data collected from various decision-makers was limited. Without enough knowledge of the SMEs using online IT systems and Cloud BI in the selected towns, it was difficult to find a large, randomised sample whose findings could be generalised to a large population outside the study units. Furthermore, there were challenges in accessing some participants who kept postponing the interview sessions, and this delayed the data collection process.

#### **8.6. Recommendations for future research**

Future studies emanating from this study could be conducting another study in all nine provinces of South Africa using randomised samples to generalise the results. To improve the framework, a longitudinal case study to evaluate its effectiveness is a potential area of future research. This would provide the researcher with ample time to study how enterprises use the framework and identify areas of improvement.

## REFERENCES

- Afolaranmi, S, Ferrer, B & Martinez-Lastra, J. 2018. A framework for evaluating security in multi-cloud environments. In: *Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. V. 1. IEEE. 3059–3066. doi.org/10.1109/IECON.2018.8591454.
- Afolayan, A & de la Harpe, A. 2019. The role of evaluation in SMMEs' strategic decision-making on new technology adoption. *Technology Analysis & Strategic Management*. 5(2):1–15. doi.org/DOI: 10.1080/09537325.2019.1702637.
- Agerfalk, PJ. 2010. Getting pragmatic. *European Journal of Information Systems*. 19(3):251–256.
- Agostino, A, Soilen, SK & Gerritsen, B. 2013. Cloud solution in business intelligence for SMEs – vendor and customer perspectives. *Journal of Intelligence Studies in Business*. 3(2013):5–28.
- Agrawal, D, Abbad, AE & Wang, S. 2011. Secure data management in the cloud. *Databases in Networked Information Systems*. 7108(2011):1-15;
- Ahmed, M & Hossain, MA. 2014. Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications*. 6(1):25–36. doi.org/10.5121/ijnsa.2014.6103.
- Ajibade, P. 2018. Technology Acceptance Model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-methods, and qualitative research. *Library Philosophy and Practice (e-journal)*. 1941(2018):1–13.
- Ajumobi, D & Kyobe, M. 2017. Alignment of human competencies with mobile phone technology and business strategies by women-led SMEs in South Africa. *Electronic Journal of Information Systems in Developing Countries*. 80(1):1–25. doi.org/10.1002/j.1681-4835.2017.tb00592.x.
- Ajzen, I. 1991. The theory of planned behaviour. *Organisational Behavior and Human Decision Processes*. 50:179–211. doi.org/10.1016/0749-5978(91)90020-T.
- Akinbi, OA. 2015. An adaptive security framework for evaluating and assessing security implementations in PaaS cloud models. EDGE HILL. Available from:

[https://repository.edgehill.ac.uk/7762/2/Akinbi Olushola - Thesis - Final - 2016.03.04.pdf](https://repository.edgehill.ac.uk/7762/2/Akinbi%20Olushola%20-%20Thesis%20-%20Final%20-%202016.03.04.pdf)  
[Accessed 21 October 2020].

- Akinola, KE & Odumosu, AA. 2015. Threat handling and security issues in cloud computing. *International Journal of Scientific and Engineering Research*. 6(11):1371–1385.
- Al-Aqrabi, H, Liu, L, Hill, R & Antonopoulos, N. 2015. Business intelligence security on the clouds: challenges, solutions and future directions. *Journal of Computer and System Sciences*. 81(1):85–96. doi.org/10.1016/j.jcss.2014.06.013.
- Al-Yaseen, HM. 2012. Challenges of implementing health care information systems in developing countries: Using a mixed-methods research. *Journal of emerging trends in computing and Information Sciences*. 3(11):1521–1529.
- Al-Yaseen, H, Eldabi, T, Lees, D & Paul, R. 2006. Operational use evaluation of IT investments : An investigation into potential benefits. *European Journal of Operational Research*. 173(3):1000–1011.
- Al-Yaseen, H, Al-Jaghoub, S, Al-Shorbaji, M & Salim, M. 2010. Post-implementation evaluation of HealthCare Information Systems in developing countries. *Information Systems Journal*. 13(1):9–16.
- Alharahsheh, H & Pius, A. 2020. A Review of key paradigms: positivism vs interpretivism. *Global Academic Journal of Humanities and Social Sciences*. 2(3):39–43. Available from: <https://www.researchgate.net/publication/338244145>.
- Alia, M, Khana, S & Vasilakos, A. 2015. Security in cloud computing: Opportunities and challenges. *Information Sciences*. 2015(305):357–384.
- Alkin, M & King, J. 2017. Definitions of evaluation use and misuse, evaluation influence, and factors affecting use. *American Journal of Evaluation*. 38(3):434–450. doi.org/DOI:10.1177/1098214017717015.
- Alliance, CS. 2015. *Best practices for mitigating risks in virtualised environments*. Available from: [https://downloads.cloudsecurityalliance.org/whitepapers/Best\\_Practices\\_for\\_Mitigating\\_Risks\\_Virtual\\_Environments\\_April2015\\_4-1-15\\_GLM5.pdf](https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf) [Accessed 15 March 2020].



- Alshamaila, Y, Papagiannidis, S & Li, F. 2013. Cloud computing adoption by SMEs in the Northeast of England: A multi-perspective framework. *Journal of Enterprise Information Management*. 26(3):250–275. doi.org/10.1108/17410391311325225.
- Amigorena, F. 2019. *Why SMBs still do not trust cloud storage providers to secure their data*. Available from: <https://www.infosecurity-magazine.com/opinions/smb-trust-cloud-storage-1-1/> [Accessed 22 November 2019].
- Anala, MR, Shetty, J & Shobha, G. 2013. A framework for secure live migration of virtual machines. In: *IEEE International Conference on Advances in Computing, Communications and Informatics*. 243–248.
- Anderson, E. 2017. *How to comply with the 5 functions of the NIST Cybersecurity Framework*. *Cyber Resilience Blog*. Available from: <https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework> [Accessed 12 May 2020].
- Ando, H, Cousins, R & Young, C. 2014. Achieving saturation in thematic analysis: development and refinement of a codebook. . *Comparative Psychology*. 2014(3):4–15.
- Angeles, S. 2013. *8 Reasons to fear cloud computing*. Available from: <https://www.businessnewsdaily.com/5215-dangers-cloud-computing.html> [Accessed 15 July 2019].
- Antoo, M, Cadessaib, Z & Gobin, B. 2015. PEST framework for analysing cloud computing adoption by Mauritian SMEs. *Lecture Notes on Software Engineering*. 3(2):107–112. doi.org/DOI: 10.7763/LNSE.2015.V3.175.
- Ashktorab, V & Taghizadeh, SR. 2012. Security threats and countermeasures in cloud computing. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. 1(2):234–245.
- Asiamah, N, Mensah, KH & Oteng-Abayie, FE. 2017. General, target, and accessible population: demystifying the concepts for effective sampling. *The Qualitative Report*. 22(6):1607–1621.
- Babbie, E. 2014. *The basics of social research*. 12th ed. Wadsworth: Cengage Learning.
- Bach, MP, Celjo, A & Zoroja, J. 2016. Technology Acceptance Model for business intelligence systems: Preliminary research. *Procedia Computer Science*. 100(2016):995–1001.

doi.org/10.1016/j.procs.2016.09.270.

- Backes, M, Grimm, N & Kate, A. 2016. Data Lineage in Malicious Environments. *IEEE Transactions on Dependable and Secure Computing*. 13(2):178–191. doi.org/10.1109/TDSC.2015.2399296.
- Bacudio, AG, Yuan, X, Chu, BT & Jones, M. 2011. An overview of penetration testing. *International Journal of Network Security & Its Applications (IJNSA)*. 3(6 November 2011):19–38.
- Balachandran, BM & Prasad, S. 2017. Challenges and benefits of deploying Big Data Analytics in the Cloud for Business Intelligence. *Procedia Computer Science*. 112(2017):1112–1122. doi.org/10.1016/j.procs.2017.08.138.
- Bam, L & Adao, V. 2019. *South Africa's SMEs should be first in line for a digital upgrade*. Available from: <https://www.weforum.org/agenda/2019/09/south-africas-smes-should-be-first-in-line-for-a-digital-upgrade/> [Accessed 23 August 2021].
- Bamba, J. 2012. *Year of Cloud BI*. Available from: <https://tdwi.org/Articles/2012/01/24/2012-Year-of-Cloud-BI.aspx?Page=1> [Accessed 20 March 2020].
- Barhatov, V, Campa, A & Pletnev, D. 2017. The impact of Internet-technologies development on small business success in Russia. *Procedia - Social and Behavioral Sciences*. 238(2018):552–561.
- Baskarada, S. 2014. Qualitative case study guidelines. *The Qualitative Report*. 19(40):1–18.
- Beever, G. 2018. *Diffusion of innovations theory: Case studies and discussion*. Available from: <https://extensionaus.com.au/extension-practice/diffusion-of-innovations-theory-case-studies-and-discussion/> [Accessed 29 October 2020].
- Behr, A. 2017. *How do you evaluate cloud service agreements and SLAs? Very carefully*. Available from: <https://www.hpe.com/us/en/insights/articles/how-do-you-evaluate-cloud-service-agreements-and-slas-very-carefully-1705.html> [Accessed 9 February 2020].
- Berdykulova, G, Sailov, A, Kaliazhdarova, S & Berdykulov, E. 2014. The Emerging Digital Economy: Case of Kazakhstan. *Procedia - Social and Behavioral Sciences*. 109(2014):1287–1291. doi.org/10.1016/j.sbspro.2013.12.626.

- Berkowsky, RW, Sharit, J & Czaja, SJ. 2017. Factors predicting decisions about technology adoption among older adults. *Innovation in Aging*. 1(3):1–12. doi.org/10.1093/geroni/igy002.
- Biesta, G. 2010. Pragmatism and the philosophical foundations of mixed methods research. In: *SAGE Handbook of Mixed Methods in Social & Behavioural Sciences*. 2nd ed. A. Tashakkori & C. Teddlie, Eds. Thousand Oaks, CA: SAGE. 95–118.
- Bignel, D. 2017. *Six hidden costs to the cloud and how to beat them*. Available from: <https://www.orange-business.com/en/blogs/connecting-technology/cloud-data-center/6-hidden-costs-to-cloud-and-how-to-beat-them> [Accessed 15 February 2020].
- Bilal, K, Malik, SU, Khan, SU & Zomaya, AY. 2014. Trends and challenges in cloud data centres. *IEEE Cloud Computing Magazine*. 1(1):10–20.
- Bills, D. 2012. *Fundamentals of Cloud Service reliability*. Available from: <https://www.microsoft.com/security/blog/2012/09/12/fundamentals-of-cloud-service-reliability/> [Accessed 24 November 2019].
- Bisong, A & Rahman, S. 2011. An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications (IJNSA)*,. 3(1):30–45.
- Bonache, J. 2021. The challenge of using a ‘non-positivist’ paradigm and getting through the peer-review process. *Human Resource Management Journal*. 31(1):37–48. doi.org/10.1111/1748-8583.12319.
- Boonsiritomachai, W, McGrath, M & Burgess, S. 2014. A research framework for the adoption of Business Intelligence by small and medium-sized enterprises. In: *27th Annual SEAAZ Proceedings for Small Enterprise Association of Australia and New Zealand Conference 16-18 July 2014*. Sidney. 16–28.
- Braun, V & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*. 2006(3):77–101. doi.org/10.1191/1478088706qp063oa.
- Braun, V & Clarke, V. 2014. What can thematic analysis offer health and wellbeing researchers? *International Journal of Qualitative Studies on Health and Well-being*. 9(2014):152–156. doi.org/DOI: 10.3402/qhw.v9.26152.

- Braun, V, Clarke, V, Hayfield, N & Terry, G. 2019. Thematic analysis. In: *Handbook of Research Methods in Health Social Sciences*. 1st ed. P. Liamputtong, Ed. Singapore: Springer. 843–860. doi.org/doi:10.1007/978-981-10-5251-4\_103.
- Brebner, P & Liu, A. 2010. Performance and cost assessment of cloud services. In: *Conference: Service-Oriented Computing - ICSOC 2010 International Workshops, PAASC, WESOA, SEE, and SOC-LOG*,. San Francisco: Schoss Dagstuhl Leibniz Centre for Informatics. doi.org/10.1007/978-3-642-19394-1.
- Brey, P. 2019. *Three hidden public cloud costs and how to avoid them*. Available from: <https://www.networkcomputing.com/cloud-infrastructure/3-hidden-public-cloud-costs-and-how-avoid-them> [Accessed 15 February 2020].
- Brezinova, M. 2013. Basic characteristics of small and medium-sized enterprises in terms of their goals. *International Journal of Business and Social Science*. 4(15):98–103.
- Brooke, S. 2019. *Is business intelligence the fastest way to improve customer experience?* Available from: <https://readwrite.com/2019/08/21/is-business-intelligence-the-fastest-way-to-improve-customer-experience.html> [Accessed 16 October 2020].
- Broughton, K. 2017. *Realizing an information security risk management framework*. Available from: <https://swimlane.com/blog/information-security-risk-management-framework/> [Accessed 16 August 2020].
- Bucur, C. 2012. Implications and directions of development of web business intelligence systems for business community. *Economic Insights – Trends and Challenges*. LXIV(2/2012):96–108.
- Budrienė, D & Zalieckaitė, L. 2012. Cloud computing application in small and medium-sized enterprises. *Issues of Business and Law*. 4(1):119–130.
- Calumpang, JC & Dilan, RE. 2016. Evaluation framework on system security requirements for Government-owned agencies in the Philippines. *International Journal of Information and Education Technology*. 6(5):398–403. doi.org/10.7763/ijiet.2016.v6.721.
- Cameron, R. 2010. Mixed methods in business and management: A call to the ‘first generation’. *Journal of Management and Organisation*. 17(2):245–267.

- Cameron, R. 2015. *Mixed Methods Research*. doi.org/10.7748/ns.29.32.41.e8858.
- Canadian Centre for Cyber Security. 2019. *Calculating robustness for boundary controls*. Available from: <https://cyber.gc.ca/sites/default/files/publications/itsp.80.032-eng.pdf> [Accessed 26 January 2020].
- Carcary, M, Doherty, E & Conway, G. 2014. The adoption of cloud computing by Irish SMEs: An exploratory study. *Electronic Journal of Information Systems Evaluation*. 17(1):3–14.
- Carson, S. 2002. Model verification and validation. In: *Proceedings of the 2002 Winter Simulation Conference*. E. Yücesan, C.. Chen, J.. Snowdon, & J.. Charnes, Eds. Marietta, GA: Brooks-PRI Automation. 52–58.
- Castleberry, A & Nolen, A. 2018. Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*. 10(6):807–815. doi.org/10.1016/j.cptl.2018.03.019.
- Cathain, AO, Murphy, E & Nicholl, J. 2007. Why, and how, mixed methods research is undertaken in health services research in England: A mixed-methods study. *BMC Health Services Research*. 7(85):1–11. doi.org/10.1186/1472-6963-7-85.
- Chan, L. 2017. *Globalization and its impacts on small businesses – it's not all bad*. Available from: <https://www.unleashedsoftware.com/blog/globalization-impacts-small-businesses> [Accessed 26 June 2020].
- Chandio, F, Burfat, F, Abro, A & Naqvi, H. 2017. Citizens' acceptance and usage of Electronic-Government services: A conceptual model of trust and technological factors. *Sindh University Research Journal-SURJ (Science Series)*. 49(3):665–668.
- Chandra, L, Seidel, S & Gregor, S. 2015. Prescriptive knowledge in IS research: Conceptualizing design principles in terms of materiality, action, and boundary conditions sciences. In: *2015 48th Hawaii International Conference on System Sciences*. IEEE Computer Society. 4039–4048.
- Chang, S, van Witteloostuijn, A & Eden, L. 2010. From the editors: Common method variance in international business research. *Journal of International Business Studies*. 41(2):178–184.
- Chang, V, Kuob, Y & Ramachandran, M. 2015. Cloud computing adoption framework: A

- security framework for business clouds. *Future Generation Computer Systems*. 57(2015):24–41.
- Chang, V, Walters, RJ & Wills, G. 2015. Cloud computing and frameworks for organisational cloud adoption. In: *Delivery and adoption of cloud computing services in contemporary organisations*. A. DeMarco, Ed. Information Science References ICG Global. 1–25. doi.org/DOI: 10.4018/978-1-4666-8210-8.ch001.
- Chao, C & Chandra, A. 2012. Impact of the owner’s knowledge of information technology (IT) on strategic alignment and IT adoption in US small firms. *Journal of Small Business and Enterprise Development*. 19(2012):114–131.
- Chen, D & Zhao, H. 2012. Data security and privacy protection issues in cloud computing. In: *International Conference on Computer Science and Electronics Engineering 23-25 March 2012*. Hangzhou. 647–651.
- Chen, H & Storey, VC. 2012. Business intelligence and analytics: From Big Data to big impact. 36(4):1165–1188.
- Chin, J, Callaghan, V & Clarke, C. 2008. End-user customisation of intelligent environments. In *the handbook of Ambient Intelligence and Smart Environments*. (June):371–407.
- Choi, M & Lee, C. 2015. Information security management as a bridge in cloud systems from private to public organizations. *Sustainability*. 7(9):12032–12051. doi.org/10.3390/su70912032.
- Chou, T. 2013. Security threats on cloud computing vulnerabilities. *International Journal of Computer Science and Information Technology (IJCSIT)*. 5(3):79–88.
- Churchill, G. 1979. A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research JMR, (pre-1986)*. 16(1):64-73.
- Clark, R. 2012. A framework for the evaluation of smart grids. In: *25th Bled eConference eDependability: Reliable and Trustworthy eStructures, eProcesses, eOperations and eServices for the Future June 17, 2012 – June 20, 2012*. Bled. 309–323.
- Clarke, R. 2012. A Framework for the evaluation of cloud sourcing proposals. In: *25th Bled eConference eDependability: Reliable and Trustworthy eStructures, eProcesses,*

- eOperations and eServices for the Future June 17-20, 2012*. Bled. 309–323.
- Clarke, V & Braun, V. 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*. 26(2):120–123.
- Claycomb, WR. 2012. *Insider Threats in the Cloud*. Available from: <https://www.acsac.org/2012/workshops/ccw/Claycomb.pdf> [Accessed 27 August 2018].
- Clohessy, T. 2017. The impact of cloud computing on IT service providers. *International Journal of Advanced Research*. 5(11):1310–1317.
- Cloud Industry Forum. 2019. *8 criteria to ensure you select the right cloud service provider*. Available from: <https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider> [Accessed 23 September 2020].
- Cloud Security Alliance. 2011. *Security guidance for critical areas of focus in cloud computing V3.0*. V. 3. doi.org/10.1016/S1353-4858(99)90042-9.
- Cloud Security Alliance. 2013. *The notorious nine. Cloud computing top threats in 2013*. Available from: <http://www.cloudsecurityalliance.org> [Accessed 31 October 2019].
- Cloud Security Alliance. 2016. *The treacherous 12 cloud computing top threats in 2016*. Available from: <http://oemhub.bitdefender.com/top-threats-to-securing-the-cloud> [Accessed 23 June 2020].
- Cloud Security White Paper. 2011. *How to evaluate the data security capabilities of cloud-based services*. Available from: [http://www.carestream.com/WhitePaper\\_Cloud-Security.pdf](http://www.carestream.com/WhitePaper_Cloud-Security.pdf) [Accessed 11 July 2011].
- Cloud Standards Customer. 2017. *Security for cloud computing: Ten steps to ensure success*. Available from: [https://www.academia.edu/21973375/Security\\_for\\_Cloud\\_Computing\\_Ten\\_Steps\\_to\\_Ensure\\_Success\\_Version\\_2\\_0](https://www.academia.edu/21973375/Security_for_Cloud_Computing_Ten_Steps_to_Ensure_Success_Version_2_0) [Accessed 7 August 2020].
- Cloud Standards Customer Council. 2016. *Cloud security standards: What to expect and what to negotiate*. Available from: <http://www.cloud-council.org/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf> [Accessed 4 July 2020].
- CloudHealth Tech Staff. 2018. *How reliable is cloud computing?* Available from:

- <https://www.cloudhealthtech.com/blog/how-reliable-is-cloud-computing> [Accessed 21 June 2019].
- Cobb, M. 2014. *Segregation of duties: Small business best practices*. Available from: <http://www.computerweekly.com/tip/Segregation-of-duties-Small-business-best-practices> [Accessed 21 August 2019].
- Cohen, L. 2019. *5 critical features for cloud security controls*. Available from: <https://techbeacon.com/security/5-critical-features-cloud-security-controls> [Accessed 7 March 2020].
- Cohen, L, Manion, L & Morrison, K. 2018. *Research Methods in Education*. 8th ed. London & New York: Routledge Taylor & Francis Group.
- Cole, R, Purao, S, Rossi, M & Sein, M. 2005. Being proactive: Where action-research meets design-research. In: *Proceedings of the 26th International Conference on Information Systems*. Las Vegas. 325–336.
- Columbus, L. 2017. *Business intelligence and analytics in the cloud*. Available from: <https://www.forbes.com/sites/louiscolumbus/2017/02/26/business-intelligence-and-analytics-in-the-cloud-2017/#7869bd0fa289> [Accessed 15 April 2020].
- Columbus, L. 2018. *The state of cloud business intelligence 2018: Why usage continues to soar*. Available from: <http://softwarestrategiesblog.com/> [Accessed 23 August 2019].
- Columbus, L. 2020. *The state of cloud business intelligence, 2020*. Available from: <https://www.forbes.com/sites/louiscolumbus/2020/04/12/the-state-of-cloud-business-intelligence-2020/?sh=2e691f9f5efd> [Accessed 2 August 2020].
- Constantinides, P, Chiasson, MW & Introna, LD. 2012. The end of information systems research: A pragmatic framework. *MIS Quarterly*. 36(1):1–19.
- Cooper, K. 2017. *Key considerations for Cloud adoption by NGOs*. Available from: <http://www.techsoup.org/support/articles-and-how-tos/key-considerations-for-cloud-adoption-by-ngos> [Accessed 12 August 2017].
- Creswell, J. 2009. *Research design: Qualitative, Quantitative and Mixed-Methods Approaches*. 2nd ed. Thousand Oaks, CA: SAGE Publications.



- Creswell, J. 2013. *Steps in Conducting a Scholarly Mixed Methods Study: What I am looking for core characteristics: Do you have a quantitative database?* Nebraska: University of Nebraska Lincoln.
- Creswell, J. 2014. *Qualitative inquiry and research design: choosing among five approaches*. 4th ed. Thousand Oaks, CA: SAGE.
- Creswell, J & Cheryl, N. 2018. *Qualitative inquiry and research design: Choosing among the five approaches*. 4th ed. Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: SAGE Publication.
- Creswell, J & Creswell, J. 2018. *Research design: Qualitative, quantitative & mixed methods approaches*. Las Vegas & New York: Sage Publication Inc.
- Creswell, J & Plano-Clark, V. 2011. *Designing and conducting mixed methods research*. 2nd ed. Thousand Oaks, CA: SAGE.
- Crocker, L. 2015. Content Validity. In: *International Encyclopedia of the Social & Behavioral Sciences*. 2nd ed. Elsevier Ltd. 774–777. doi.org/https://doi.org/10.1016/B978-0-08-097086-8.44011-0.
- Dabrowska, E & Cornford, T. 2001. Evaluation and Telehealth: An interpretative study. In: *Proceedings of the Thirty-Fourth Annual Hawaii International Conference on System Sciences (HICSS)-34 June 2001*. N. Piscataway, Ed. Maui, Hawaii: Computer Society Press of the IEEE. 200–220.
- Dawson, L & Van Belle, JP. 2013. Critical success factors for business intelligence in the South African financial services sector. *South African Journal of Information Management*. 15(1):545–557.
- DeCarlo, A. 2011. *The need for cloud computing security standards*. Available from: <https://searchsecurity.techtarget.com/magazineContent/The-need-for-cloud-computing-security-standards> [Accessed 21 October 2019].
- Decker, R, Haltiwanger, J, Jarmin, R & Miranda, J. 2016. Where has all the skewness gone? The decline in high-growth (young) firms in the US. *European Economic Review*. 86(2016):4–23.

- Deepa, G & Thilagam, PS. 2016. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. *Information and Software Technology*. 74(2016):160–180.
- Denzin, N & Lincoln, Y. 2011. *The Sage handbook of qualitative research*. 4th ed. Los Angeles, CA: Sage Publications.
- Devesh, K, Samalia, HV & Verma, P. 2017. Exploring the suitability of cloud computing for small and medium-sized enterprises in India. *Journal of Small Business and Enterprise Development*. 24(4):814–832. doi.org/10.1108/JSBED-01-2017-0002.
- Dhar, S. 2014. From outsourcing to cloud computing: Evolution of information technology services. *Management Research Review*. 35(8):664–675. doi.org/http://dx.doi.org/10.1108/01409171211247677.
- Dholakiya, P. 2016. *The 4 biggest business-intelligence challenges facing entrepreneurs*. Available from: <https://www.entrepreneur.com/article/280432> [Accessed 21 January 2020].
- Dresner, H. 2017. *Cloud computing and business intelligence market study licensed to domo*. Available from: <https://www.domo.com/blog/wp-content/uploads/2018/04/2018-Wisdom-of-Crowds-Cloud-Computing-BI-Market-Study-Licensed-to-Do.pdf> [Accessed 29 April 2020].
- Dudharejia, M. 2018. *Four major challenges of adopting cloud business intelligence – and how to overcome them*. Available from: <https://www.cloudcomputing-news.net/news/2018/jun/11/four-major-challenges-adopting-cloud-business-intelligence-and-how-overcome-them/> [Accessed 21 August 2019].
- Durcevic, S. 2019. *10 Cloud computing risks & challenges businesses are facing these days*. Available from: <https://www.datapine.com/blog/cloud-computing-risks-and-challenges/> [Accessed 13 February 2020].
- Durg, K & Podder, S. 2020. *Navigating the interoperability challenge in multi-cloud environments*. Available from: <https://www.accenture.com/us-en/blogs/cloud-computing/kishore-durg-cloud-interoperability-challenges> [Accessed 29 August 2020].
- Dyczkowski, M, Korczak, J & Dudycz, H. 2014. Multi-criteria evaluation of the intelligent dashboard for SME managers based on scorecard framework. *Business Informatics*.

3(33):46–60. doi.org/10.15611/ie.2014.3.04.

Edirisingha, P. 2012. *Interpretivism and Positivism (Ontological and Epistemological Perspectives)*. Available from: <https://prabash78.wordpress.com/2012/03/14/interpretivism-and-positivism-ontological-and-epistemological-perspectives/> [Accessed 22 November 2017].

Edwards, J. 2009. Cutting through the fog of cloud security. *Computerworld*. 43(8):26–30.

Eldabi, T, Paul, R & Sbeih, H. 2008. Post-implementation evaluation of IT systems: A close review of practice. In: *Evaluating Information Systems: Public and Private Sector*. Z. Irani & P. Love, Eds. Oxford: Linacre House & Jordan Hill. 134–152.

Elena, G & Johnson, CW. 2015a. Lay people's and experts' risk perception of cloud computing services. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*. 5(4):1–19.

Elena, G & Johnson, CW. 2015b. Factors influencing risk acceptance of cloud computing services in the UK Government. *International Journal on Cloud Computing: Services and Architecture*. 5(2):312–328. doi.org/DOI : 10.5121/ijccsa.2015.53011.

Elmalah, K & Nasr, M. 2019. Cloud business intelligence. *International Journal in Advanced Networking and Applications*. 10(6):4120–4124.

Elsanhouri, AE, Ahmed, MA & Abdullah, AH. 2012. Cloud applications versus web applications: A differential study. In: *INNOV 2012: The First International Conference on Communications, Computation, Networks and Technologies*. 31–36.

Ereth, J & Dahl, D. 2013. Business intelligence in the cloud: Fundamentals for a service-based evaluation concept. *CEUR Workshop Proceedings*. 1049:1–20.

Eriksson, P & Kovalainen, A. 2015. *Qualitative methods in business research: A practical guide to social research*. 2nd ed. Thousand Oaks, California: SAGE Publications Ltd.

eSentire Managed Security Services. 2012. *Cloud-based security checklist*. Available from: <http://02f9c3b.netsolhost.com/blog1/wp-content/uploads/Cloudsecurity.pdf> [Accessed 22 October 2019].

Etikan, I, Sulaiman, AM & Rukayya, SA. 2016. Sampling, comparison of convenience and

- purposive sampling. *American Journal of Theoretical and Applied Statistics*. 5(1):1–4.
- Ettlie, J. 1980. Adequacy of stage models for decisions on adoption of innovation. *Psychological Reports*. 46(3):991–995.
- Ettlie, J & Penner-Hahn, DJ. 1994. Adoption complexity and economies of scope for new process technology in manufacturing. *The Journal of High Technology Management Research*. 5(1):171–182.
- European Union Agency for Network and Information Security. 2015. *Security framework for governmental clouds*. doi.org/10.2824/57349.
- Evelson, B & Bennett, M. 2017. *Enterprise BI platforms with majority on-premises deployments, Q3 2017: A significant reshuffling of vendor positions in a changing landscape key takeaways*. Available from: <https://www.budgetingsolutions.co.uk/wp-content/uploads/2020/09/Forrester-Enterprise-BI-Platforms-On-Premise.pdf> [Accessed 24 July 2019].
- Evens, T, De Marez, L & Schuurman, D. 2008. Adoption versus use diffusion: Predicting User Acceptance of Mobile TV in Flanders. In: *ICE-B 2008: International Conference on e-Business: Proceedings. July 26-29, 2008*. B. Shishkov & M. van Sinderen, Eds. Porto, Portugal: INSTICC PRESS. 123–132.
- Farbey, B, Land, F & Target, D. 1992. Evaluating investments in IT. *Journal of Information Technology*. 7(2):109-122.
- Farjoun, M, Ansell, C & Boin, A. 2015. Pragmatism in organization studies: Meeting the challenges of a dynamic and complex world. *Organization Science*. 26(6):1787–1804.
- Fernandes, D, Soares, L, Gomes, J, Freire, M & Inacio, P. 2014. Security issues in cloud environments: A survey. *International Journal of Information Security (IJIS)*. 2014(1):1–62.
- Fichman, R & Kemerer, C. 2012. Adoption of software engineering process innovations: The case of object-orientation. *Sloan Management Review*. 34(2):7–19.
- FindLaw Attorney Writers. 2018. *Cloud computing and the law: The basics*. Available from: <https://technology.findlaw.com/networking-and-storage/cloud-computing-and-the-law-the-basics.html> [Accessed 18 February 2020].

- Fitzpatrick, BW & Lueck, JJ. 2010. The case against data lock-in. *Commun. ACM*. 53(11):42–46. doi.org/10.1145/1839676.1839691.
- Flack, C. 2016. IS Success Model for Evaluating Cloud Computing for Small Business Benefit: A Quantitative Study. *Doctor of Business Administration Dissertations*.
- Foley, M & Lardner, L. 2015. *Drafting and negotiating effective cloud computing agreements*. Available from: <https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/posts/drafting-and-negotiating-effective-cloud-computing-agreements> [Accessed 9 February 2020].
- Frambach, R & Schillewaert, N. 2002. Organisational innovation adoption: A multi-level framework of determinants and opportunities for future research. *Journal of Business Research*. 55(2):163–176.
- Fry, A, Ryley, T & Thring, R. 2018. The influence of knowledge and persuasion on the decision to adopt or reject alternative fuel vehicles. *Sustainability (Switzerland)*. 10(9):1–20. doi.org/10.3390/su10092997.
- Gadia, S. 2018. *How to manage five key cloud computing risks*. Available from: <https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf> [Accessed 2 December 2019].
- Gajajiva, A. 2019. *Data security in cloud computing: who's in charge?* Available from: <https://www.matillion.com/resources/blog/data-security-in-cloud-computing-whos-in-charge/> [Accessed 7 March 2020].
- Gardner, B. 2014. *Cost of a data breach. Building an Information Security Awareness Program*,. doi.org/doi:10.1016/b978-0-12-419967-5.00003-x.
- Gartner. 2016. *Applying a ' Cloud-First ' checklist to ensure successful sourcing and Business-IT alignment*. Available from: <https://www.gartner.com/en/documents/3277826/applying-a-cloud-first-checklist-to-ensure-successful-so> [Accessed 15 November 2018].
- Geer, D & Sullivan, P. 2019. *Building the best incident response framework for your enterprise*. Available from: <https://searchsecurity.techtarget.com/tip/Incident-response-frameworks-for-enterprise-security-teams> [Accessed 1 October 2019].

- Gendron, MS. 2014. *Business Intelligence and the Cloud: Strategic implementation guide*. New Jersey: John Wiley & Sons, Incorporated.
- Gentles, SJ, Charles, C, Ploeg, J & McKibbin, K. 2015. Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*. 20(11):1772–1789.
- Ghaffari, K, Delgosha, MS & Abdolvand, N. 2014. Towards cloud computing: A SWOT analysis on its adoption in SMEs. *International Journal of Information Technology Convergence and Services*. 4(2):13–20. doi.org/10.5121/ijitcs.2014.4202.
- Ghobakhloo, M, Sabouri, MS, Hong, TS & Zulkifli, N. 2011. Information technology adoption in small and medium-sized enterprises: An appraisal of two decades literature. *Interdisciplinary Journal of Research in Business*. 1(7):53–80.
- Gioia, D, Corley, K & Hamilton, A. 2013. Seeking qualitative rigour in inductive research notes on the Gioia methodology. *Organisational Research Methods*. 16(1):15–31.
- Gleeson, NC & Walden, I. 2014. ‘It’s a jungle out there’: Cloud computing, standards and the law. *European Journal of Law and Technology*. 5(2):1–22. doi.org/10.2139/ssrn.2441182.
- Golafshani, N. 2003. Understanding reliability and validity in qualitative research. *The Qualitative Report*. 8(4):597–607.
- Goldkuhl, G. 2008. *What kind of pragmatism in Information Systems research?* Available from: <https://pdfs.semanticscholar.org/d643/1e41eec4c16ce104bde9404fb87ec39c4fa0.pdf> [Accessed 28 November 2017].
- Goldkuhl, G. 2012. Pragmatism versus interpretivism in qualitative information systems research. *European Journal of Information Systems*. 21(2):135–146.
- Goles, T & Hirschheim, R. 2012. The Paradigm is dead, the Paradigm is dead...long live the paradigm: The legacy of Burrell and Morgan. *The International Journal of Management Science*. 28(1):249–268.
- Govender, NM & Pretorius, M. 2015. A critical analysis of information and communications technology adoption: The strategy-as-practice perspective. *Acta Commercii*. 15(1):1–13. doi.org/10.4102/ac.v15i1.229.
- Grabova, O, Darmont, J, Chauchat, JH & Zolota, I. 2010. Business intelligence for small and

- middle-sized enterprise. *Special Interest Group on Management of Data (SIGMOD) Record*. 39(2):231–245.
- Graham, L. 2017. *Ransomware can cost firms over \$700,000; cloud computing may provide the protection they need*. Available from: <https://www.cnn.com/2017/08/04/cloud-computing-cybersecurity-defend-against-ransomware-hacks.html> [Accessed 16 August 2020].
- Gralewski, P. 2017. *Four critical steps to align data protection and cloud strategy*. Available from: <https://www.commvault.com/4-critical-steps-to-align-data-protection-and-cloud-strategy> [Accessed 23 February 2020].
- Granneman, J. 2014. *IT security frameworks and standards: Choosing the right one*. Available from: <http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one> [Accessed 23 June 2015].
- Granneman, J. 2019. *Top 7 IT security frameworks and standards explained*. Available from: <https://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one%0A> [Accessed 12 August 2020].
- Gray, DE. 2013. *Doing research in the real world. Theoretical perspectives and research methodologies*. Los Angeles: SAGE Publications.
- Green, P. 2009. *Industrialisation in South Africa: The impact of globalisation*. Available from: <https://philmgreen.files.wordpress.com/2010/08/industrialisation-in-south-africa.pdf> [Accessed 24 December 2020].
- Greene, T. 2010. *How to check on your cloud provider*. Available from: <https://www.networkworld.com/article/2197086/how-to-check-on-your-cloud-provider.html> [Accessed 8 February 2020].
- Greenhalgh, T, Robert, G, Macfarlane, F, Bate, P & Kyriakidou, O. 2004. Diffusion of innovations in service organizations: systematic review and recommendations. *The Milbank Quarterly*. 82(4):581–629.
- Greer, MB. 2010. *Survivability and information assurance in the cloud*. Available from: <http://download.101com.com/GIG/Custom/Stand/Cloud/LMSurvivabilityInformationAssuranceinCloud.pdf> [Accessed 4 December 2019].

- Greis, J. 2014. *Building trust in the cloud Creating confidence in your cloud ecosystem*. Available from: [https://www.ey.com/Publication/vwLUAssets/EY\\_-\\_Building\\_trust\\_in\\_the\\_cloud/\\$FILE/EY-grc-building-trust-in-the-cloud.pdf](https://www.ey.com/Publication/vwLUAssets/EY_-_Building_trust_in_the_cloud/$FILE/EY-grc-building-trust-in-the-cloud.pdf) [Accessed 27 September 2019].
- De Groot, J. 2019. *What is data classification? A data classification definition*. Available from: <https://digitalguardian.com/blog/what-data-classification-data-classification-definition> [Accessed 29 February 2020].
- Guarda, T, Santos, M, Pinto, F, Augusto, M & Silva, C. 2013. Business intelligence as a competitive advantage for SMEs. *International Journal of Trade, Economics and Finance (IJTEF)* 2013. 4(4):187–190.
- Guest, G, MacQueen, K & Namey, E. 2012. *Applied thematic analysis*. Los Angeles: Sage Publications.
- Gupta, A & Kaur, K. 2013. Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology*. 4(3):328–333.
- Gurjar, S & Rathore, V. 2013. Cloud business intelligence is what business need today. *International Journal of Recent Technology and Engineering*. 1(6):81–86.
- Hai, LC & Alam-Kazmi, S. 2015. Dynamic support of governments in online shopping. *Asian Social Science*. 11(22):1–9.
- Haji, K, Mohd, S & Abd, Z. 2015. Barriers and drivers in cloud ERP adoption among SMEs. *Journal of Information Systems Research and Innovation*. 9(1):9–20.
- Hallikainen, P & Chen, L. 2005. A holistic framework on information systems evaluation with a case analysis. *The Electronic Journal Information Systems Evaluation*. 9(2):57–64.
- Hamida, A, Razakb, F, Bakar, A, Salihin, W & Abdullah, W. 2016. The effects of perceived usefulness and perceived ease of use on continuance intention to use e-government. *Procedia Economics and Finance*. 35(2016):644–649. doi.org/DOI: 10.1016/S2212-5671(16)00079-4.
- Hamshire, H, Spearing, R & Wibberley, C. 2013. What are reasonable expectations? Healthcare student perceptions of their programmes in the North West of England. *Nurse Education*



*Today*. 33(2):173–179.

- Harfoushi, O, Alfawwaz, B, Ghatasheh, NA, Obiedat, R, Abu-Faraj, MM & Faris, H. 2014. Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review. *Communications and Network*. 06(01):15–21. doi.org/10.4236/cn.2014.61003.
- Harrison, S, Tzounis, A, Maglaras, L, Siewe, F & Janicke, H. 2016. A security evaluation framework for UK E-Government services using agile software development. *International Journal of Network Security & Its Applications (IJNSA)*. 8(2):51–69.
- Hasbini, A. 2019. *It's time to take ransomware attacks seriously*. Available from: <https://www.bizcommunity.com/Article/196/661/193789.html> [Accessed 20 September 2011].
- Hashim, HS & Hassan, Z Bin. 2015. Factors that influence the users' adoption of cloud computing services at Iraqi Universities: An empirical study. *Australian Journal of Basic and Applied Sciences*. 9(2015):379–390.
- Hashizume, K, Rosado, D, Fernández-ME & Fernandez, E. 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*. 4(5):1–13. doi.org/DOI: 10.1186/1869-0238-4-5.
- Hatwar, S V & Chavan, R. 2015. Cloud computing security issues and countermeasures. *International Journal of Computer Applications*. 119(17):46–53.
- Hauser, A, Eggers, F & Güldenber, S. 2020. Strategic decision-making in SMEs: effectuation, causation, and the absence of strategy. *Small Business Economics*. 54(3):775–790. doi.org/10.1007/s11187-019-00152-x.
- Hayes, KJ, Eljiz, K, Dadich, A, Fitzgerald, J & Sloan, T. 2015. Trialability, observability and risk reduction accelerating individual innovation adoption decisions. *Journal of Health Organization and Management*. 29(2):271–294. doi.org/10.1108/JHOM-08-2013-0171.
- Hazell, L. 2014. *Data Separation in Cloud*. Available from: <https://cybersecuritynews.co.uk/data-separation-in-cloud-computing/> [Accessed 4 December 2019].
- Heang, R. 2017. *The needs and challenges of adopting business intelligence for small and medium-sized enterprise (SME)*. Available from: <http://www.diva->

portal.org/smash/get/diva2:1080914/FULLTEXT01.pdf [Accessed 13 August 2020].

- Heiser, J. 2019. *How to evaluate cloud service provider security*. Available from: <https://www.gartner.com/doc/3275117/evaluate-cloud-service-provider-security> [Accessed 5 December 2019].
- Henning, E, Van Rensburg, W & Smit, B. 2006. *Qualitative researching beyond tools and techniques. Finding your way in qualitative research*. Pretoria: Van Schaik.
- Herwig, V & Friess, K. 2016. Integrating business intelligence services in the Cloud: A conceptual model. In: *Business Intelligence: Concepts, methodologies, tools and applications*. 1st ed. M. Khosrow-Pour, Ed. Hershey: IGC Global. 572–584. doi.org/DOI: 10.1037/a0018784.
- Hooda, A. 2014. Business intelligence over the cloud. *International Journal of Management (IJM)*. 5(2):90–100.
- Horakova, M & Skalska, H. 2013. Business intelligence and implementation in a small enterprise. *Journal of Systems Integration*. 2013(2):50–61.
- Horst, M, Kuttschreuter, M & Gutteling, J. 2007. Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Human Behaviour*. 23(4):1838–1852.
- Hretcanu, C. 2015. Current trends in the knowledge economy. *Ecoforum Journal*. 4(2):170–175.
- Huang, J & Nicol, DM. 2013. Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*. 2(9):1–14.
- Hughes, AS. 2016. Mixed-methods research. *Observer*. 29(5):234–241.
- Hulin, C, Netemeyer, R & Cudeck, R. 2001. Can a Reliability Coefficient Be Too High? *Journal of Consumer Psychology*. 10(1):55–58.
- Hurtaud, S & de la Vaissière, L. 2017. *How to ensure control and security when moving to SaaS/cloud applications*. Available from: [https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu\\_ensure-control-security-saas-cloud-applications\\_07102014.pdf](https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu_ensure-control-security-saas-cloud-applications_07102014.pdf) [Accessed 3 October 2018].
- Hurtaud, S, de la Vaissière, L & Aboukir, Y. 2017. *The aftermath of ransomware*. Available from: <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-aftermath-of->

ransomware-112017.pdf [Accessed 22 November 2019].

- Hussain, W, Hussain, F, Hussain, O, Bagia, R & Chang, E. 2018. Risk-based framework for SLA violation abatement from the cloud service provider's perspective. *Computer Journal*. 61(9):1306–1322. doi.org/10.1093/comjnl/bxx118.
- Hussein, NH & Khalid, A. 2016. A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security*. 14(1):52–56.
- IBM Security. 2020. *Cost of a Data Breach Report 2020*. Available from: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/> [Accessed 2 August 2020].
- Ibrahim, O & Musah, A. 2015. Small and medium enterprises (SMEs) in the cloud in developing countries: A synthesis of the literature and future research directions. *Journal of Management and Sustainability*. 5(1):115–139.
- Igli, T & Solange, G-H. 2019. Information security evaluation: A holistic approach. In: *The management of technology series*. 1st ed. C. Aghroum, Ed. Boca Raton: Taylor and Francis Group, LLC. 55–70.
- Indriasari, E, Prabowo, H, Meyliana, K & Hidayanto, AN. 2018. Key benefits of cloud business intelligence: A systematic literature review. *International Journal of Mechanical Engineering and Technology (IJMET)*. 9(13):819–831.
- Information Security Forum. 2016. *Standard of good practice for information security*. Available from: <https://www.securityforum.org/uploads/2016/07/SoGP-2016-Exec-Summary-FINAL-260716.pdf> [Accessed 26 June 2020].
- Iqbal, S, Kiah, L, Anuar, N, Daghighi, B, Wahab, A & Khan, S. 2016. Service delivery models of cloud computing: security issues and open challenges. *Security and Communication Networks*. 5(June):422–437. doi.org/10.1002/sec.
- ISACA. 2011. *IT control objectives for cloud computing: Controls and assurance in the cloud*. Available from: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx> [Accessed 15 June 2020].

- Izrailevsky, Y & Bell, C. 2018. Cloud Reliability. *IEEE Cloud Computing*. 5(3):39–44. doi.org/10.1109/MCC.2018.032591615.
- Jabbar, MA, Saleem, MAM, Gebreselassie, S & Beyene, H. 2003. Role of knowledge in the adoption of new agricultural technologies: An approach and an application. *International Journal of Agricultural Resources, Governance and Ecology*. 2(3–4):312–327. doi.org/10.1504/ijarge.2003.003974.
- Jakimoski, K. 2016. Security techniques for data protection in cloud computing. *International Journal of Grid and Distributed Computing*. 9(1):49–56.
- Jansen, R, Curşeu, P, Vermeulen, P, Geurts, J & Gibcus, P. 2013. Information processing and strategic decision-making in small and medium-sized enterprises: the role of human and social capital in attaining decision effectiveness. *International Small Business Journal*. 31(2):192–216. doi.org/DOI: 10.1177/0266242611406762.
- Javaid, MA. 2014. Implementation of Cloud Computing for SMEs. *World Journal of Computer Application and Technology*. 2(3):66–72. doi.org/10.13189/wjcat.2014.020302.
- Jebreen, I. 2012. Using Inductive Approach a s Research Strategy in Requirements Engineering. *International Journal of Computer and Information Technology*. 1(2):162–172.
- Jelonek, D & Wysłocka, E. 2014. Barriers to the development of cloud computing adoption and usage in SMEs in Poland. *Advances in Information Science and Applications*. I(1):128–133.
- Johnson, J, Yasugi, S, Sugino, Y, Pranata, S & Shen, S. 2018. Person re-identification with the fusion of hand-crafted and deep pose-based body region features. *International Journal of Higher Education*. 6(5):26–41. doi.org/10.5430/ijhe.v6n5p26.
- de Jongh, P, Janette Larney, J, Mare, E, van Vuuren, F & Verster, T. 2017. A proposed best practice model validation framework for banks. *South African Journal of Economic and Management Sciences*. 20(1):1–15.
- Juan-Verdejo, A & Baars, H. 2013. Decision support for partially moving applications to the cloud: The example of business intelligence. In: *The 2013 International Workshop on Hot Topics in Cloud Services*. 35–42.
- Kasem, M & Hassanein, E. 2014. Cloud business intelligence survey. *International Journal of*

- Computer Applications*. 90(1):307–317. doi.org/10.1007/978-3-319-11460-6\_26.
- Kaur, K & Vashisht, S. 2013. Data separation issues in cloud computing. *International Journal for Advance Research in Engineering and Technology*. 1(X):26–29.
- Kaur, K, Azad, N & Singh, P. 2013. Cost-effective cloud-based business intelligence model for small scale organizations. *International Journal of Computer Applications*. 63(8):24–30.
- Kaushik, V & Walsh, CA. 2019. Pragmatism as a research paradigm and its implications for Social Work research. *Social Sciences*. 8(9):3–17. doi.org/10.3390/socsci8090255.
- Kazim, M & Zhu, SY. 2015. A survey on top security threats in cloud computing. *International Journal of Applied Computer Science and Applications*. 6(3):10495–10500. doi.org/10.14569/IJACSA.2015.060316.
- Kazmi, R, Ghani, I, Mohamad, R & Tariq, M. 2016. Trade-off between automated and manual testing : A production possibility curve cost model. *International Journal of Advanced Software Computer Application*. 8(1):12–27.
- Keesee, G & Shepard, M. 2011. Perceived attributes predict course management system adopter status. *Online Journal of Distance Learning Administration*. IV(I):35–49.
- Kelley, D & Warren, L. 2015. *Practical legal considerations when thinking about cloud computing*. Available from: <https://ccbjournal.com/articles/practical-legal-considerations-when-thinking-about-cloud-computing> [Accessed 21 February 2020].
- Kelly, L & Cordeiro, M. 2020. Three principles of pragmatism for research on organizational processes. *Methodological Innovations*. 1(2):1–10. doi.org/DOI:10.1177/2059799120937242.
- Kerravala, Z. 2019. *When it comes to uptime, not all cloud providers are created equal*. Available from: <https://www.networkworld.com/article/3394341/when-it-comes-to-uptime-not-all-cloud-providers-are-created-equal.html> [Accessed 23 December 2020].
- Kersten, J. 2018. *Who's responsible for cloud security?* Available from: <https://kirkpatrickprice.com/blog/whos-responsible-cloud-security/> [Accessed 17 August 2019].
- Khan, SA. 2012. Security assessment framework: a complexity perspective. *International Journal*

*of Information and Education Technology*. 2(5):439–441.

- Khan, N & Al-Yasiri, A. 2015. Framework for cloud computing adoption: a roadmap for SMEs to cloud migration. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*. 5(56):258–269. doi.org/Vol. 5, DOI : 10.5121/ijccsa.2015.5601.
- Khanagha, S, Volberda, H, Sidhu, J & Oshri, I. 2013. Management innovation and adoption of emerging technologies: The case of cloud computing. *European Management Review*. 10(5):1–67.
- Khorshed, T, Ali, ABMS & Wasimi, SA. 2012. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*. 28(6):833–851. doi.org/10.1016/j.future.2012.01.006.
- Kikawa, CR. 2019. A statistical analysis of business intelligence acceptance by SMEs in the City of Tshwane, Republic of South Africa. *Academy of Entrepreneurship Journal*. 25(2):1–19.
- Kit, E. 1995. *Software Testing in the Real World: Improving the Process*. Reading, MA: Addison-Wesley.
- Kodagali, S. 2019. *17 Security criteria to look at when evaluating a cloud service*. Available from: <https://www.skyhighnetworks.com/cloud-security-blog/17-security-criteria-to-look-at-when-evaluating-a-cloud-service/%0A> [Accessed 7 December 2019].
- Koops, BJ & Goodwin, M. 2014. *Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law*. Available from: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2698263](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263) [Accessed 23 January 2017].
- Koparkar, P & Mackrell, D. 2015. How fluffy is the cloud?: Cloud business intelligence for a not-for-profit organisation. In: *In ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*. Association for Information System. Adelaide. 1–10. doi.org/https://arxiv.org/ftp/arxiv/papers/1606/1606.00752.pdf.
- KPMG. 2016. *Moving to the cloud – key considerations*. Available from: <https://home.kpmg.com/content/dam/kpmg/pdf/2016/04/moving-to-the-cloud-key-risk-considerations.pdf> [Accessed 23 September 2019].
- Krippendorff, K. 2013. *Content analysis. An introduction to its methodology*. 3rd ed. California,

CA: Sage Publications.

- Kubicek, H & Cimander, R. 2009. Three dimensions of organizational interoperability. Insights from recent studies for improving interoperability frame-works. *European Journal of ePractice*. 2009(3):1–12.
- Kumar, A. 2018. *Ten key challenges in cloud computing and how to overcome*. Available from: <https://it.toolbox.com/blogs/ankitkumar/10-key-challenges-in-cloud-computing-and-how-to-overcome-110518> [Accessed 20 September 2012].
- Kumar, S & Padmapriya, S. 2014. A survey on cloud computing security threats and vulnerabilities. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*. 2(1):622–625. doi.org/10.1109/ICCS.2012.6.
- Kupsch, JA, Miller, BP, Heymann, E & Cesar, E. 2010. First principles of vulnerability assessment. In: *17th ACM Conference on Computer and Communications Security*. Association for Computing Machinery New York NY. 87–92. doi.org/https://doi.org/10.1145/1866835.1866852.
- Kyobe, M, Namirembe, E & Shongwe, M. 2015. The alignment of information technology applications with non-technological competencies of SMEs in Africa. *The Electronic Journal of Information Systems in Developing Countries*. 67(5):1–22.
- Labes, S, Repschläger, J, Zarnekow, R, Stanik, A & Kao, O. 2012. Standardization approaches within Cloud Computing: Evaluation of infrastructure as a service architecture. In: *Proceedings of the Federated Conference on Computer Science and Information Systems*. 923–930. doi.org/978-83-60810-51-4.
- Lacey, D & James, BE. 2010. *Review of availability of advice on security for small and medium-sized organisations*. Available from: <https://ico.org.uk/media/about-the-ico/documents/1042344/review-availablility-of-security-advice-for-sme.pdf> [Accessed 10 November 2019].
- Lacity, M & Reynolds, P. 2014. Cloud services practices for small and medium-sized enterprises. *MIS Quarterly Executive*. 13(1):31-44.
- Lai, P. 2017. The literature review of technology adoption models and theories for novelty technology. *Journal of Information Systems and Technology Management*. 14(1):21–38.

doi.org/10.4301/S1807-17752017000100002.

- Lamb, J. 2016. Post-publication review. *Australasian Journal of Information Systems*. 20(2016):1–5.
- Lechesa, M, Seymour, L & Schuler, J. 2012. ERP Software-as-Service (SaaS): Factors affecting adoption in South Africa. In: *5th Working Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS): Lecture Notes in Business Information Processing, LNBIP-105 Re-conceptualizing Enterprise Information Systems*. W. Aalst, J. Mylopoulos, M. Rosemann, M. Shaw, C. Szyperski, C. Møller, & S. Chaudhry, Eds. Berlin, Heidelberg: Springer. 152–167.
- Ledwaba, L & Makgahlela, L. 2017. The value of information resources in sustaining SMME projects in Limpopo Province. In: *The 2nd Annual Conference on "The Independence of African States in the Age of Globalisation" 26 - 28 July 2017*. M. Sebola & J. Tsheola, Eds. Tlotlo Hotel, Gaborone, Botswana: International Conference on Public Administration & Development Alternatives (IPADA). 156–163.
- Leedy, P & Ormrod, J. 2015. *Practical research planning and design*. 11th ed. Pretoria: Pearson Education Ltd.
- Leitch, CM, Hill, FM & Harrison, RT. 2010. The philosophy and practise of interpretivist research in entrepreneurship: Quality, validation, and trust. *Organizational Research Methods*. 13(1):67–84.
- Lewis, GA. 2012. The role of standards in cloud-computing interoperability [Technical notes]. In: *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. 1652–1661. doi.org/10.1109/HICSS.2013.470.
- Li, H, Liang, P, Yang, J & Chen, S. 2010. Analysis of cloud-based security vulnerability assessment. In: *E-Business Engineering, IEEE International Conference*. Los Alamitos, CA, USA. 490–494.
- Llave, M. 2017. Business intelligence and analytics in small and medium-sized enterprises: A systematic literature review. *Procedia Computer Science*. 121(2017):194–205. doi.org/10.1016/j.procs.2017.11.027.
- Llave, MR. 2019. Business Intelligence and Analytics in Small and Medium-sized Enterprises: A



- Systematic Literature Review. *International Journal of Business Intelligence Research*. 10(1):19–41. doi.org/DOI: 10.4018/IJBIR.2019010102.
- Luís, J, Erdmann, A, Hörner, B & Meirelles, S. 2020. Integrating quantitative and qualitative data in mixed-methods research. *Scielo*. 26(3):1–9.
- Mabotja, L. 2019. Are South African Manufacturing SMMEs ready for the Fourth Industrial Revolution? *Journal of Education and Vocational Research, AMH International*. 9(2):20–26. doi.org/DOI: 10.22610/jevr.v9i2(V).2798.
- Maguire, M & Delahunt, B. 2017. Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *Ireland Journal of teaching and learning in Higher Education*. 3(3):250–275.
- Mahajan, A & Sharma, S. 2015. The malicious insiders threat in the cloud. *International Journal of Engineering Research and General Science*. 3(2):245–256.
- Mairura, K. 2016. Relative Advantage as a Determinant of Technology Adoption among Automobile Mechanics in Micro and Small Enterprises in Kenya. *IOSR Journal Of Humanities And Social Science (IOSR-JHSS)*. 21(1):86. Available from: [www.iostrjournals.org](http://www.iostrjournals.org).
- Majhi, SK & Dhal, SK. 2016. A study on security vulnerability on cloud platforms. In: *Physics Procedia*. V. 78. doi.org/10.1016/j.procs.2016.02.010.
- Malak, J. 2016. *An analysis of the technological, organizational, and environmental factors influencing cloud adoption*. Available from: <https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=3948&context=dissertations> [Accessed 23 May 2019].
- Malik, A & Nazir, MM. 2012. Security framework for cloud computing environment: A literature review. *Journal of Emerging Trends in Computing and Information Sciences*. 3(3):390–394.
- Manekar, S & Pradeepini, G. 2017. Opportunity and challenges for migrating Big Data Analytics in Cloud. In: *IOP Conference Series: Materials Science and Engineering*. doi.org/10.1088/1757-899X/225/1/012148.
- Marko, K. 2018. *Consider costs when selecting a cloud deployment model*. Available from:

<https://searchcloudcomputing.techtarget.com/tip/Consider-costs-when-selecting-a-cloud-deployment-model> [Accessed 31 January 2020].

Marquis, H. 2018. *Why you need to treat cloud computing as a new business model?* Available from: <https://www.globalknowledge.com/us-en/resources/case-studies/why-you-need-to-treat-cloud-computing-as-a-new-business-model/> [Accessed 20 March 2020].

Marshall, C & Rossman, G. 2014. *Designing qualitative research*. 6th ed. London: SAGE Publications Ltd.

Mashandudze, E & Dwolatzky, B. 2015. Major challenges impeding the fast adoption of cloud computing: A case study of South African organisations and emerging economics. *Open Journal of Mobile Computing and Cloud Computing*. 2(1):1–18.

Mashingaidze, S. 2014. Descriptive business intelligence analysis: cutting edge strategic asset for SMEs, is it really worth it? *Journal of Governance and Regulation*. 3(4):70–83.

Matikiti, R, Mpinganjira, M & Roberts-lombard, M. 2018. Application of the technology acceptance model and the Technology Organisation Environment Model to examine social media marketing use in the South African Tourism Industry. *South African Journal of Information Management*. 20(1):168–179.

Maxwell, JA. 2013. *Qualitative research design: An interactive approach*. 3rd ed. Thousand Oaks, CA: Sage.

McLeod, S. 2013. *What is validity?*. *Simply Psychology*. Available from: <https://www.simplypsychology.org/reliability.html> [Accessed 9 August 2020].

Meijer, SS, Catacutan, D, Ajayi, OC, Sileshi, GW & Nieuwenhuis, M. 2015. The role of knowledge, attitudes and perceptions in the uptake of agricultural and agroforestry innovations among smallholder farmers in sub-Saharan Africa. *International Journal of Agricultural Sustainability*. 13(1):40–54. doi.org/10.1080/14735903.2014.912493.

Menon, L, Rehani, B & Gund, S. 2012. Business intelligence on the cloud: Overview and use cases. *International Journal of Computer Application*. 2012(1):25–30.

Mesbahi, M, Rahmani, A & Hosseinzadeh, M. 2018. Reliability and high availability in cloud computing environments : a reference roadmap. *Human-centric Computing and Information*

*Sciences*. 8(20):3–31. doi.org/10.1186/s13673-018-0143-8.

- Mihas, P, Creswell, J & Plano-Clark, V. 2019. Learn to use an exploratory sequential mixed method design for instrument development. In: *SAGE Research Methods Datasets Part 2*. Thousand Oaks: SAGE Publications, Ltd. 55–71.
- Miller, Z. 2017. The Enduring Use of the Theory of Planned Behavior. *Human Dimensions of Wildlife*. 22(6):583–590. doi.org/https://doi.org/10.1080/10871209.2017.1347967.
- Mirai Security. 2019. *Security Frameworks for Small Enterprise*. Available from: <https://www.miraisecurity.com/blog/security-frameworks-for-small-enterprise> [Accessed 3 August 2020].
- Mkansi, M & Acheampong, EA. 2012. Research philosophy debates and classifications: Students' dilemma. *The Electronic Journal of Business Research Methods*. 10(2):132–140.
- Mndzebele, N. 2013. The Effects of Relative Advantage, Compatibility and Complexity in the Adoption of EC in the Hotel Industry. *International Journal of Computer and Communication Engineering*. 2(4):473–476. doi.org/10.7763/ijcce.2013.v2.229.
- Modi, C, Patel, D, Borisaniya, B, Patel, A & Rajarajan, M. 2013. A survey on security issues and solutions at different layers of Cloud computing. *Journal of Supercomputing*. 63(2):561–592. doi.org/10.1007/s11227-012-0831-5.
- Modimogale, L & Kroeze, JH. 2009. Using ICTs to become a competitive SME in South Africa. In: *13th International Business Information Management Association Conference (13th IBIMA)*. 504–513.
- Moen, K & Middelthon, A. 2015. Qualitative research methods. In: *Research in Medical and Biological Sciences*. 2nd ed. P. Laake, H.B. Benestad, & B.R. Olsen, Eds. Academic Press. 321–378. doi.org/https://doi.org/10.1016/B978-0-12-799943-2.00010-0.
- Mogull, R, Arlen, J & Gilbert, F. 2017. *The security guidance for critical areas of focus in cloud computing v4.0*. Available from: <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf> [Accessed 23 January 2021].
- Mohlameane, M & Ruxwana, N. 2013. The potential of cloud computing as an alternative

- technology for SMEs in South Africa. *Journal of Economics, Business and Management*. 1(4):396–400. doi.org/DOI: 10.7763/JOEBM.2013.V1.85.
- Mohlameane, M & Ruxwana, N. 2014. The awareness of cloud computing: A case study of South African SMEs. *International Journal of Trade, Economics and Finance*. 5(1):1–6.
- Mohlameane, M & Ruxwana, N. 2020. Exploring the impact of cloud computing on existing South African regulatory frameworks. *South African Journal of Information Management*. 22(1):1–9.
- Momani, AM & Jamous, MM. 2017. The evolution of technology acceptance theories. *International Journal of Contemporary Computer Research (IJCCR)*. 1(1):51–58. doi.org/10.1002/anie.201003816.
- Moore, J. 2014. *Business intelligence takes to the cloud for small businesses*. Available from: [https://www.cio.com/article/3237786/business-intelligence/9-ways-youre-failing-at-business-intelligence.html#tk.drr\\_mlt](https://www.cio.com/article/3237786/business-intelligence/9-ways-youre-failing-at-business-intelligence.html#tk.drr_mlt) [Accessed 12 February 2018].
- Moraetes, G. 2018. *Choosing the right security framework to fit your business*. Available from: <https://securityintelligence.com/choosing-the-right-security-framework-to-fit-your-business/> [Accessed 7 June 2020].
- Morgan, D. 2014a. Pragmatism as a paradigm for social research. *Qualitative Inquiry*. 20(8):1045–1053.
- Morgan, D. 2014b. *Integrating qualitative and quantitative methods: A pragmatic approach*. Thousand Oaks, CA: SAGE.
- Morgan, D. 2020. Pragmatism as a basis for grounded theory. *Qualitative Report*. 25(1):64–73.
- Morgan, D & Nica, A. 2020. Iterative Thematic Inquiry: A New Method for Analyzing Qualitative Data. *International Journal of Qualitative Methods*. 19(2):1–11. doi.org/10.1177/1609406920955118.
- Morneau, T. 2019. *Seven cloud service evaluation criteria to help you choose the right cloud service provider*. Available from: <https://www.threatstack.com/blog/7-cloud-service-evaluation-criteria-to-help-you-choose-the-right-cloud-service-provider> [Accessed 26 January 2020].

- Mortimer, K & Laurie, S. 2019. Partner or supplier: An examination of client/agency relationships in an IMC context. *Journal of Marketing Communications*. 25(1):28–40. doi.org/10.1080/13527266.2017.1391861.
- Müller, K & Roodt, G. 2013. Content validation: The forgotten step-child or a crucial step in assessment centre validation? *South African Journal of Industrial Psychology*. 39(1):12–29. doi.org/http://dx.doi.org/10.4102/sajip.v39i1.1153.
- Mussa, M, Kipanyula, MJ, Angello, C & Sanga, CA. 2016. Evaluation of livestock information network knowledge system based on user satisfaction definition of Information System Evaluation. *International Journal of Information and Communication Technology Research*. 6(8):115–130.
- Mwika, D, Banda, A, Chembe, C & Kunda, D. 2018. The impact of globalisation on SMEs in emerging economies: A case study of Zambia. *International Journal of Business and Social Science*. 9(3). doi.org/doi:10.30845/ijbss.v9n3p6.
- Myers, MD. 2009. *Qualitative research in business and management*. London: Sage Publications.
- Myers, MD. 2020. *Qualitative research in Information Systems*. London: SAGE Publication.
- Myers, MD & Avison, DE. 2011. Qualitative research in Information Systems. *Management Information systems Quarterly*. 21(2):241–242.
- Nachmias, CF & Nachmias, D. 2008. *Research methods in the social sciences*. 7th ed. New York: Worth.
- Al Nadab, Z. 2017. *A validation framework for an online English Language Exit Test : A case study using Moodle as an assessment management system*. Available from: [https://espace.library.uq.edu.au/data/UQ\\_702967/s43349920\\_final\\_thesis.pdf?](https://espace.library.uq.edu.au/data/UQ_702967/s43349920_final_thesis.pdf?) [Accessed 23 July 2019].
- Namey, E, Guest, G, McKenna, K & Chen, M. 2016. Evaluating bang for the buck: a cost-effectiveness comparison between individual interviews and focus groups based on thematic saturation levels. *American Journal of Evaluation*. 37(3):425–40.
- National Computing Centre Group. 2018. *The hidden cost of cloud failure*. Available from: <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2019/november/the->

hidden-cost-of-cloud-failure/ [Accessed 16 July 2020].

- National Institute of Standards and Technology. 2020. *Cyber security framework: Uses and benefits of the framework*. Available from: <https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework> [Accessed 8 March 2021].
- Nenzhelele, T & Pellissier, R. 2014. Competitive intelligence implementation challenges of small and medium-sized enterprises. *Mediterranean Journal of Social Sciences*. 5(16):92–99.
- Ngeru, J & Bardhan, TK. 2015. Selecting cloud deployment model using a Delphi Analytic Hierarchy process. *Industrial and Systems Engineering Review*. 3(1):59–70.
- Niehaves, B & Plattfaut, R. 2014. Internet adoption by the elderly: Employing IS technology acceptance theories for understanding the age-related digital divide. *European Journal of Information Systems*. 23(6):708–726. doi.org/19.
- Van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*. 20(2017):113–132.
- Niselow, T. 2018. *Five massive data breaches affecting South Africans*. Available from: <https://www.news24.com/fin24/companies/ict/five-massive-data-breaches-affecting-south-africans-20180619-2> [Accessed 2 August 2020].
- Novakouski, M & Lewis, GA. 2012. *Interoperability in the E-Government*. Pittsburgh, PA: Carnegie Mellon University.
- Nowell, L, Norris, J, White, D & Moules, N. 2017. Thematic analysis striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*. 16(1):1–13. doi.org/<https://doi.org/10.1177/1609406917733847>.
- Nyalungu, V. 2011. The application of a business intelligence tool for strategic planning in a higher education institution : A case study of the University of the Witwatersrand. *TD : The Journal for Transdisciplinary Research in Southern Africa*. 7(1):53–72.
- Nyoro, M, Kamau, J, Wanyembi, G, Titus, W & Dinda, W. 2015. Review of Technology Acceptance Model usage in predicting e-commerce adoption. *International Journal of Application or Innovation in Engineering & Management*. 4(1):46–49.
- Oates, JB. 2006. *Researching Information Systems and Computing*. London: Sage Publications

Ltd.

- Ocloo, CE, Akaba, S & Worwui-Brown, DK. 2014. Globalization and competitiveness: challenges of small and medium enterprises (SMEs) in Accra, Ghana. *International Journal of Business and Social Science*. 5(4):287–296.
- Olawale, F & Garwe, D. 2010. Obstacles to the growth of new SMEs in South Africa: A principal component analysis approach. *Management, African Journal of Business*. 4(5):729–738.
- Olbrich, S, Poppelbub, J & Niehaves, B. 2012. Critical contextual success factors for business intelligence: A Delphi study on their relevance, variability, and controllability. In: *45th Hawaii International Conference on System Sciences, Hawaii, USA, January 4–7, 2012*. Hawaii. 4148–4157.
- Olexova, C. 2014. Business intelligence adoption: a case study in the retail chain. *World Scientific and Engineering Academy and Society Transactions on Business and Economics*. 11(2014):97–106.
- Olise, MC, Anigbogu, TU, Edoko, TD & Okoli, MI. 2014. Determinants of ICT adoption for improved SME's performance in Anambra State, Nigeria. *American International Journal of Contemporary Research*. 4(7):164–176.
- Oliveira, T & Martins, MF. 2011. Literature review of information technology adoption models at the firm level. *The Electronic Journal Information Systems*. 14(1):110–121.
- Olszak, C. 2014. Business Intelligence in Cloud. *Polish Journal of Management Studies*. 10(2):116–127.
- Olszak, C & Ziemba, E. 2004. Business intelligence systems as a new generation of decision support systems. In: *Proceedings PISTA 2004, International Conference on Politics and Information Systems: Technologies and Applications*. Orlando, The Internatio.
- Olszak, C & Ziemba, E. 2007. Approach to building and implementing business intelligence systems. *Interdisciplinary Journal of Information, Knowledge, and Management*. 2(2007):135–148.
- Olszak, C & Ziemba, E. 2012. Critical success factors for implementing business intelligence systems in small and medium enterprises on the example of Upper Silesia. *Interdisciplinary*

*Journal of Information, Knowledge, and Management*. 7(2012):15–26.

- Olszewska, M, Heidenberg, J, Weijola, M, Mikkonen, K & Porres, I. 2016. Quantitatively measuring a large-scale agile transformation. *Journal of Systems and Software*. 2016(117):258–273.
- Olushola, T & Abiola, J. 2017. The efficacy of technology acceptance model: A review of applicable theoretical models in Information Technology researches. *Quest Journals Journal of Research in Business and Management*. 4(11):70–83.
- Omaid, A. 2015. Selecting the appropriate study design for your research: Descriptive study designs. *Journal of Health Specialties*. 3(3):153. doi.org/10.4103/1658-600x.159892.
- Ong, JW, Ismail, H Bin & Goh, GGG. 2012. The competitive advantage of small and medium enterprises (SMEs): the role of entrepreneurship and luck. *Journal of Small Business and Entrepreneurship*. 23(3):373–391. doi.org/10.1080/08276331.2010.10593491.
- Opara-Martins, J, Sahandi, R & Tian, T. 2016. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing Advances, Systems and Applications*. 5(2016):1–18. doi.org/DOI: 10.1186/s13677-016-0054-z.
- Oracle White Paper. 2010. *Cloud-ready business intelligence with Oracle IIg*. Available from: <http://www.oracle.com/us/solutions/business-intelligence/cloud-ready-oracle-bi-177505.pdf> [Accessed 15 April 2019].
- Osborn, E. 2014. *Business versus technology: Sources of the perceived lack of cyber security in SMEs*. Oxford, UK: University of Oxford.
- Osorio-Gallego, CA, Londono-Metaute, JH & Lopez-Zapata, E. 2016. Analysis of factors that influence ICT adoption by SMEs in Colombia. *Intangible Capital*. 12(2):666–732. doi.org/10.3926/ic.726.
- Owusu, A. 2020. Determinants of Cloud Business Intelligence Adoption Among Ghanaian SMEs. *International Journal of Cloud Applications and Computing*. 10(4):48–69. doi.org/10.4018/ijcac.2020100104.
- Oza, N, Karppinen, K & Savola, R. 2010. User experience and security in the cloud – An empirical



- study in the Finnish cloud consortium. In: *2nd IEEE International Conference on Cloud Computing Technology and Science*. 621–628. doi.org/10.1109/CloudCom.2010.114.
- Pant, P. 2009. *Business intelligence (BI): How to build a successful BI strategy?* Available from: [http://www.loria.fr/~ssidhom/UE909R/1\\_BI\\_strategy.pdf](http://www.loria.fr/~ssidhom/UE909R/1_BI_strategy.pdf) [Accessed 25 June 2020].
- Pantić, Z & Babar, MA. 2019. *Guidelines for building a private cloud infrastructure*. Available from: <http://nexgsd.org/wp-content/uploads/2012/05/Guidelines-to-BuildingPrivateCloud-Infrastructure-Technical-Report.pdf> [Accessed 18 April 2020].
- Papachristodoulou, E, Koutsaki, M & Kirkos, E. 2017. Business intelligence and SMEs: Bridging the gap. *Journal of Intelligence Studies in Business*. 7(1):70–78.
- Patel, H & Connolly, R. 2007. Factors influencing technology adoption: A review. In: *Information Management in the Networked Economy: Issues and Solutions - Proceedings of the 8th International Business Information Management Association Conference, IBIMA 2007*. International Business Information Management Association, IBIMA. 416–431.
- Pathirage, CP, Amaratunga, RDG & Haigh, RP. 2016. The role of philosophical context in the development of research methodology and theory. *The Built and Human Environment Review*. 1(1):10–29.
- Patil, S & Chavan, R. 2020. Cloud business intelligence: An empirical study. *Studies in Indian Place Names UGC Care Journal*. 40(27):747–754.
- Patrick, S. 2015. *The small business fear of the cloud - debunked*. Available from: <https://www.cloudcomputing-news.net/news/2015/nov/25/small-business-fear-cloud-debunked/> %0A [Accessed 22 November 2019].
- Patton, M. 2015. *Qualitative research and evaluation methods*. 4th ed. Los Angeles: Sage.
- Paulinus, WI & David, E. 2013. Framework for sustainable management of public housing estates in Nigeria. *Journal of US-China Public Administration*. 10(10):934–944.
- Pearson, S & Benameur, A. 2011. Privacy, security and trust issues arising from cloud computing. In: *2nd IEEE International Conference on Cloud Computing Technology and Science*. Computer Society. doi.org/10.1109/CloudCom.2010.66.
- Peltier, J, Zhao, Y & Schibrowsky, J. 2012. Technology adoption by small businesses: an

- exploratory study of the interrelationships of the owner and environmental factors. *International Small Business Journal*. 30(4):406–31.
- Perkins, J. 2016. *Information security policy*. Available from: <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/information-security-policy/isp.pdf> [Accessed 26 October 2017].
- Phneah, E. 2013. *SaaS integration challenges pose security risks*. Available from: <https://www.zdnet.com/article/saas-integration-challenges-pose-security-risks/> [Accessed 4 October 2020].
- Phocas Software. 2015. *What is cloud business intelligence (Cloud BI)?* Available from: <https://www.phocassoftware.com/business-intelligence-blog/what-is-cloud-business-intelligence-cloud-bi> [Accessed 7 October 2018].
- Pirttimaki, VH. 2010. Conceptual analysis of business intelligence. *South African Journal of information management*. 9(2):1–10.
- Podsakoff, PM, MacKenzie, SB, Lee, JY & Podsakoff, NP. 2003. Common method biases in behavioural research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*. 88(5):879–903. doi.org/10.1037/0021-9010.88.5.879.
- Ponelis, SR. 2015. Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of Information Systems research in small and medium enterprises. *International Journal of Doctoral Studies*. 10(2015):535–550.
- Potgieter, P. 2019. The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at the Central University of Technology. In: *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019*. V. 12. K. Njenga, Ed. Kalpa Publications in Computing. 272–262. doi.org/10.29007/gprf.
- Pratt, MK & Fruhlinger, J. 2019. *What is business intelligence? Transforming data into business insights*. Available from: <https://www.cio.com/article/2439504/business-intelligence-definition-and-solutions.html> [Accessed 7 March 2020].
- Preece, A & Bularafa, M. 2015. Community of inquiry method and language skills acquisition:

- empirical evidence. *Journal of Education and Practice*. 6(27):89–93.
- Punch, K. 2013. *Introduction to social research: Quantitative and qualitative approaches*. London: Sage Publications Ltd.
- Radatz, J, Geraci, A & Katki, F. 1990. *IEEE standard glossary of software engineering terminology*. New York, NY: The Institute of Electrical and Electronics Engineers.
- Rafique, S, Humayun, M, Gul, Z, Abbas, A & Javed, H. 2015. A systematic review of web application security development model. *Journal of Computer and Communications*. 43(2):259–276. doi.org/10.1007/s10462-012-9375-6.
- Rahayu, R & Day, J. 2015. Determinant factors of e-commerce adoption by SMEs in a developing country: Evidence from Indonesia. *Procedia - Social and Behavioral Sciences*. 195(2015):142–150. doi.org/10.1016/j.sbspro.2015.06.423.
- Rahman, S. 2017. The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “ testing and assessment ” research: A literature review. *Journal of Education and Learning*. 6(1):102–112. doi.org/10.5539/jel.v6n1p102.
- Ramachandran, M & Chang, V. 2016. Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management*. 36(4):618–625. doi.org/10.1016/j.ijinfomgt.2016.03.005.
- Ramgovind, S, Eloff, M & Smith, E. 2010. The management of security in cloud computing. In: *Information Security for South Africa (ISSA), 2010*. 1–7. doi.org/10.1109/ISSA.2010.5588290.
- Ranjan, J. 2014. Business intelligence: Concepts, components, techniques and benefits. *Journal of Theoretical and Applied Information Technology*. 9(1):60–70.
- Rayome, A. 2019. *How to choose the right cybersecurity framework*. Available from: <https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/> [Accessed 6 December 2019].
- Raza, M. 2013. *What are the hidden costs of cloud adoption?* Available from: <http://blogs.bmc.com/cloud-adoption-costs/?print=pdf> [Accessed 16 February 2020].
- Raza, M. 2018. *Reliability vs availability: What’s the difference?* Available from:

<https://www.bmc.com/blogs/reliability-vs-availability/> [Accessed 15 June 2019].

- Ren, M. 2019. Why technology adoption succeeds or fails: an exploration from the perspective of intra-organizational legitimacy. *Journal of Chinese Sociology*. 6(21):1–26. doi.org/10.1186/s40711-019-0109-x.
- Renfro, NA & Smith, JL. 2016. *Threat/vulnerability assessments and risk analysis*. Available from: <https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis> [Accessed 18 February 2017].
- Renny, Guritno, S & Siringoringo, H. 2013. Perceived usefulness, ease of use, and attitude towards online shopping usefulness towards online airlines ticket purchase. *Procedia - Social and Behavioral Sciences*. 81:212–216. doi.org/10.1016/j.sbspro.2013.06.415.
- Rezaei, R, Chiew, T & Lee, S. 2013. A review of interoperability assessment models. *Journal of Zhejiang University-SCIENCE C (Computers & Electronics)*. 14(9):663–681. doi.org/10.1631/jzus.C1300013.
- Richardson, M. 2017. *Four steps to more effective data management*. Available from: <https://www.smeweb.com/2017/08/31/sme-efficient-data-management/> [Accessed 25 February 2020].
- Ristov, S, Gusev, M & Kostoska, M. 2012. Cloud computing security in business information systems. *International Journal of Network Security & Information Technologies Applications (IJNSA)*. 4(2):131–140. doi.org/DOI: 10.5121/ijnsa.2012.4206 75.
- Rivastava, H & Kumar, S. 2015. Data security framework for secure cloud computing. *Journal of Information Security*. 6(2016):12–23.
- Rizvi, S, Ryoo, J, Kissell, J, Aiken, W & Liu, Y. 2018. A security evaluation framework for cloud security auditing. *Journal of Supercomputing*. 74(11):5774–5796. doi.org/10.1007/s11227-017-2055-1.
- Robinson, N, Valeri, L, Cave, J, Starkey, T, Graux, H, Reese, S & Hopkins, P. 2010. *The cloud understanding the security, privacy and trust challenges*. Available from: [http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010\\_en.pdf](http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf) [Accessed 11 November 2016].

- Rogers, E. 1995. *Diffusion of innovations*. 2nd ed. New York: Free Press.
- Rogers, E. 2003. *Diffusion of innovations*. 3rd ed. New York: Free Press.
- Rogers, E. 2005. *Diffusion of innovations*. 5th ed. New York: Free Press.
- Romes, R. 2015. *The benefits and risks of cloud computing*. Available from: <http://www.claconnect.com/resources/articles/the-benefits-and-risks-of-cloud-computing> [Accessed 2 December 2019].
- Rostek, K, Wiśniewski, M & Kucharska, A. 2012. Cloud business intelligence for smes consortium. *Foundations of Management*. 4(1):105–122. doi.org/10.2478/fman-2013-0006.
- Roulston, K. 2014. Conducting and analyzing individual interviews. In: *The Oxford handbook of qualitative research in American music education*. C.M. Conway, Ed. Oxford: Oxford University Press. 250–270.
- Roulston, K. 2018. *How to develop an interview guide (Part 1)*. Available from: <https://qualpage.com/2018/02/08/how-to-develop-an-interview-guide-part-1> [Accessed 27 April 2019].
- Rouse, M. 2011. *Software-as-a-Service BI (SaaS BI)*. Available from: <http://searchbusinessanalytics.techtarget.com/definition/Software-as-a-Service-BI-SaaS-BI>, [Accessed 26 February 2019].
- Rubin, H & Rubin, I. 2012. *Qualitative interviewing: The art of hearing data*. 3rd ed. Los Angeles: Sage.
- Rupra, S, Karie, N & Rabah, K. 2018. A framework for assessing security in a SaaS Cloud paradigm for SMEs. *Mara International Journal of Scientific & Research Publications*. 2(2):1–14.
- Rykiel, EJ. 1996. Testing ecological models: the meaning of validation. *Ecological Modelling*. 90(3):29–244.
- Sabi, HM, Uzoka, FME, Langmia, K & Njeh, FN. 2016. Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management*. 36(2):183–191.
- Sadler, GR, Lee, HC, Lim, RSH & Fullerton, J. 2010. Recruitment of hard-to-reach population

- subgroups via adaptations of the snowball sampling strategy. *Nursing and Health Sciences*. 12(3):369–374. doi.org/10.1111/j.1442-2018.2010.00541.x.
- Sadoughi, F, Ali, O & Erfannia, L. 2019. Evaluating the factors that influence cloud technology adoption: A comparative case analysis of health and non-health sectors: A systematic review. *Health Informatics Journal*. 33(2):1–29. doi.org/10.1177/1460458219879340.
- Sahandi, R, Alkhalil, A & Opara-Martins, J. 2012. SMES' perception of cloud computing: potential and security. *Journal of Information Technology Management*. 380(1):186–195.
- Sahin, I. 2006. A detailed review of Rogers' Diffusion of Innovations Theory and Educational Technology-related studies Based on Rogers' theory. *The Turkish Online Journal of Educational Technology (TOJET)*. 5(2:3):14–25.
- Salim, A, Li, M, He, Q & Shen, J. 2016. Cloud computing services adoption in Australian SMEs: A firm-level investigation. In: *Pacific Asia Conference on Information Systems 2016 Proceedings*. United States: AIS Electronic Library. 1–11.
- Salim, S, Sedera, D, Sawang, S & Alarifi, A. 2014. Technology adoption as a multi-stage process. *Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014*. (January 2016).
- Salim, S, Sedera, D, Sawang, S, Alarifi, A & Atapattu, M. 2015. Moving from evaluation to trial: How do SMEs start adopting Cloud ERP? *Australasian Journal of Information Systems*. 2015(19):219–254.
- Salum, KH, Zaidi, M & Rozan, A. 2016. Exploring the challenge impacted SMEs to adopt cloud ERP. *Indian Journal of Science and Technology*. 9(45):1–8. doi.org/10.17485/ijst/2016/v9i45/100452.
- Sangar, BA & Iahad, AN. 2013. Critical factors that affect the success of business intelligence systems implementation in an organization. *International Journal of Scientific & Technology Research*. 2(2):25–35.
- Sanjay, RA & Vijayaraj, M. 2011. Analysis of the characteristics and trusted security of cloud computing. *International Journal on Cloud Computing: Services and Architecture*. 1(3):61–69. doi.org/10.5121/ijccsa.2011.1305.

- Santos-olmo, A, Sánchez, LE, Caballero, I, Camacho, S & Fernandez-medina, E. 2016. The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*. 8(30):1–27. doi.org/10.3390/fi8030030.
- Sargent, R. 1984. A tutorial on verification and validation of simulation models. In: *Proceedings of the 1984 Winter Simulation Conference*. S. Sheppard, U. Pooch, & U. Pegden, Eds. IEEE. 115–122.
- Sargent, R. 2011. Verification and validation of simulation models. In: *Proceedings of the 2011 Winter Simulation Conference*. S. Jain, R. Creasey, J. Himmelspach, K. White, & M. Fu, Eds. Phoenix, Arizona: Piscataway, N.J.: IEEE. 183–198.
- Saunders, M, Lewis, P & Thornhill, A. 2012. *Research methods for business students*. 6th ed. Cape Town: Pearson Education Limited.
- Schaefer, T, Hofmann, M, Loos, P & Fettke, P. 2014. Feature selecting the right cloud operating model privacy and data security in the cloud. *ISACA JOURNAL*. 3(2014):112–19.
- Schiff, J. 2016. *Experience, How to use BI to improve the customer*. Available from: <https://www.cio.com/article/3042805/how-to-use-bi-to-improve-the-customer-experience.html> [Accessed 16 October 2020].
- Scholz, P, Scieder, C, Kurze, C, Gluchowski, P & Boehringer, M. 2010. Benefits and challenges of business intelligence adoption in small and medium-sized enterprises. In: *18th European Conference on Information Systems*. 1–12.
- Schoonenboom, J & Johnson, RB. 2017. How to construct a mixed methods research design. *KZfSS Kolner Zeitschrift für Soziologie und Sozialpsychologie*. 60(2):107–131. doi.org/10.1007/s11577-017-0454-1.
- Scott, LM. 2016. Theory and research in construction education: the case for pragmatism. *Construction Management and Economics*. 34(7–8):552–560. doi.org/10.1080/01446193.2016.1151539.
- Seidman, I. 2012. *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. 4th ed. New York: Teachers College.
- Sekaran, U & Bougie, R. 2012. *Research methods for business: A skill building approach*. 5th ed.

Chichester: John Wiley and Sons.

- Sen, J. 2013. Security and privacy issues in cloud computing. *Architectures and Protocols for Secure Information Technology*. 3(5):42. doi.org/10.1109/HICSS.2011.103.
- Senarathna, I, Yeoh, W, Warren, M & Salzman, S. 2016. Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs. *Australasian Journal of Information Systems* . 20(2016):1–20. doi.org/10.3127/ajis.v20i0.1193.
- Sentilles, S, Papatheocharous, E & Ciccozzi, F. 2018. What do we know about software security evaluation? A preliminary study. In: *6th International Workshop on Quantitative Approaches to Software Quality (QuASoQ)*. 30–37.
- Shahbazi, A, Brinkley, J & Tabrizi, K. 2013. A distributed key based security framework for private clouds. *International Journal of Advanced Computer Science and Applications(IJACSA)*. 4(9):79–83.
- Shaikh, R & Sasikumar, M. 2015. Data classification for achieving security in cloud computing. *Procedia Computer Science*. 45(C):493–498. doi.org/10.1016/j.procs.2015.03.087.
- Sharda, R, Delen, D & Turban, E. 2015. *Business intelligence and analytics: Systems for decision support*. 10th ed. New York: Pearson.
- Sharma, R, Apoorva, S, Madireddy, V & Jain, V. 2008. Best practices for communication between client and vendor in IT outsourcing projects. *Journal of Information, Information Technology, and Organizations*. 3(2):061–093. doi.org/10.28945/131.
- Sheikh, A. 2011. SaaS BI: Sustainable business intelligence solution for SMBs. *International Journal of Research in Finance & Marketing*. 3(1):210–217.
- Sherman, R. 2015. *How to evaluate and select the right BI tools*. Available from: <https://searchbusinessanalytics.techtarget.com/feature/How-to-evaluate-and-select-the-right-BI-analytics-tool> [Accessed 30 September 2018].
- Sheshaaayee, A & Swetha, M. 2015. The challenges of business intelligence in cloud computing. *Indian Journal of Science and Technology*. 8(36):211–225.
- Shimamoto, CD. 2015. *How to evaluate cloud security?* Available from:



<https://www.techsoup.org/support/articles-and-how-tos/how-to-evaluate-cloud-security>  
[Accessed 20 August 2020].

- Shuaibu, B, Norwawi, N, Selamat, M & Al-Alwani, A. 2015. Systematic review of web application security development model. *Artificial Intelligence Review*. 43(2):259–276. doi.org/10.1007/s10462-012-9375-6.
- Shukla, S, Agarwal, S & Shukla, A. 2012. Trends in Cloud-ERP for SMB 's : A Review. *International Journal of New Innovations in Engineering and Technology (IJNIET)*. 1(1):7–11.
- da Silva, C, da Silva, J, Rodrigues, R, Nascimento, L & Garcia, V. 2013. Systematic mapping study on security threats in cloud computing. *International Journal of Computer Science and Information Security*. 11(3):55–64.
- Silverman, D. 2010. *Qualitative research*. London: Sage.
- Simorjay, F. 2014. *Data classification for cloud readiness*. Available from: <https://download.microsoft.com/download/0/A/3/0A3BE969-85C5-4DD2-83B6-366AA71D1FE3/Data-Classification-for-Cloud-Readiness.pdf> [Accessed 1 March 2020].
- Small Enterprise Development Agency. 2020. *SMME Quarterly Update 3rd Quarter 2019*. Available from: [http://www.seda.org.za/Publications/Publications/SMME Quarterly 2017-Q3.pdf](http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%202017-Q3.pdf) [Accessed 20 January 2021].
- Sniehotta, F, Presseau, J & Araújo-Soares, V. 2014. Time to retire the theory of planned behaviour. *Health Psychology Review*. 8(1):1–7. doi.org/DOI: 10.1080/17437199.2013.869710.
- Solanki, S & Nabeel, S. 2014. Cloud computing: Data separation issues. *International Journal & Magazine of Engineering, Technology, Management and Research*. 1(11):155–160.
- Song, Z. 2013. *A decision support system for application migration to the Cloud*. Available from: <http://elib.unistuttgart.de/opus/volltexte/2013/8262/> [Accessed 26 January 2020].
- Soofi, AA, Khan, MI & Amin, F. 2014. A review on data security in cloud computing. *International Journal of Computer Applications*. 94(12):12–20.
- Soong, C & Lam, C. 2015. *Report on Hong Kong SME cloud adoption, security & privacy readiness survey*. Hong Kong.

- South African Government Gazette No.42304 Department of Small Business Development. 2019. *Revised Schedule 1 of the National Definition of Small Enterprise in South Africa*. South Africa.
- Stanton, B & Theofanos, MF. 2018. *Navigating the Cloud: A usability framework*. Available from: <https://uxpamagazine.org/navigating-the-cloud/> [Accessed 30 January 2020].
- Staten, J. 2013. *How to avoid the hidden costs of cloud computing*. Available from: <https://www.zdnet.com/article/how-to-avoid-the-hidden-costs-of-cloud-computing/> [Accessed 16 February 2020].
- Straub, E. 2017. Understanding technology adoption: Theory and future directions for informal learning. *Review of Educational Research*. 79(2):625–649. doi.org/10.3102/0034654308325896.
- Subashini, S & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*. 34(1):1–11. doi.org/10.1016/j.jnca.2010.07.006.
- Subramanian, N & Jeyaraj, A. 2018. Recent security challenges in cloud computing. *Computers and Electrical Engineering*. 71(July 2017):28–42. doi.org/10.1016/j.compeleceng.2018.06.006.
- Sweetman, M. 2019. *4 best cloud deployment models*. Available from: <https://luneba.com/blog/cloud-deployment-models> [Accessed 31 January 2020].
- Symantec Corporation. 2014. *Internet security threat report*. V. 19. Available from: [http://www.symantec.com/content/en/us/enterprise/other\\_resources/b-istr\\_main\\_report\\_v19\\_21291018.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf) [Accessed 23 June 2018].
- Taherdoost, H. 2018. A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*. 22(2018):960–967. doi.org/10.1016/j.promfg.2018.03.137.
- Takahashi, D. 2018. *What kind of sensitive data is in the cloud?* Available from: <https://venturebeat.com/2018/04/15/mcafee-26-of-companies-have-suffered-cloud-data-theft/> [Accessed 20 April 2020].
- Tamer, C, Kiley, M, Ashrafi, N & Kuilboer, JP. 2013. Risks and benefits of business intelligence

in the cloud. In: *In Proceedings of the Northeast Decision Sciences Institute Annual Meeting*, 86. 3–10.

Tan, C, Hassali, M, Saleem, F, Shafie, A, Aljadhay, H & Gan, V. 2015. Building intentions with the theory of planned behaviour: A qualitative assessment of salient beliefs about pharmacy value added services in Malaysia. *Health Expectations*. 19(1):1215–1225. doi.org/doi:10.1111/hex.12416.

Teddlie, C & Tashakkori, A. 2009. *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences*. New York: SAGE Publications.

Tembedza, W. 2012. *Assessing legal risks in the move to the cloud*. Available from: <https://www.bizcommunity.com/Article/196/547/192787.html> [Accessed 18 February 2020].

The University of Leicester. 2015. *Policy for Selection and Use of Cloud Services Version & Status: ROI*. Available from: <https://www2.le.ac.uk/offices/itservices/downloads/policies/selection-and-use-of-cloud-services/selection-and-use-of-cloud-services> [Accessed 22 October 2019].

Thompson, WJ & van der Walt, JS. 2010. Business intelligence in the cloud, 2017. *South African Journal of Information Management*. 12(1):13–17. doi.org/10.4102/sajim.v12i1.445.

Thong, JYL. 1999. An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems*. 15(4):187–214. doi.org/10.2307/40398410.

Timans, R, Wouters, P & Heilbron, J. 2019. Mixed methods research: what it is and what it could be. *Theory and Society*. 48(2):193–216. doi.org/10.1007/s11186-019-09345-5.

Timperley, B. 2017. *How South African's SMEs can solve the connectivity conundrum*. Available from: <https://www.itweb.co.za/content/XnWJadMb8wKvbjO1> [Accessed 21 December 2020].

Tiwari, A. 2010. *Information Security Risk Management: An Overview Risk Management: An Essential Guide to Protecting Critical Assets*. Available from: <http://www.suite101.com/profile.cfm>. [Accessed 28 September 2020].

- Tiwari, PK & Mishra, B. 2012. Cloud computing security issues, challenges and solution. *International Journal of Emerging Technology and Advanced Engineering*. 2(8):306–310.
- Tofan, DC. 2011. Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*. 3(3):128–135. doi.org/10.1002/mus.22142.
- Tripp, O, Pistoia, M, Cousot, P, Cousot, R & Guarnieri, S. 2013. Andromeda: Accurate and scalable security analysis of web applications. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 7793 LNCS:210–225. doi.org/10.1007/978-3-642-37057-1\_15.
- Turner, G. 2018. *How technology is reshaping South Africa's small business economy*. Available from: <https://www.xero.com/content/dam/xero/pdf/southafrica-tech-adoption-report.pdf> [Accessed 15 November 2020].
- Turyakira, P. 2018. Ethical practices of small and medium-sized enterprises in developing countries: A literature analysis. *South African Journal of Economic and Management Sciences*. 21(1):145–153.
- Tutunea, MF & Rus, VR. 2014. Business intelligence solutions for SMEs. *Procedia Economics and Finance*. 2(2012):865–870.
- UK Essays. 2015. *Understanding research philosophy: Why is it important sociology essay?* Available from: <https://www.ukessays.com/essays/sociology/understanding-research-philosophy-why-is-it-important-sociology-essay.php?cref=1> [Accessed 21 November 2017].
- UK Essays. 2018a. *Globalisation: Threats and benefits for SMEs*. Available from: <https://www.ukessays.com/essays/economics/the-benefits-and-threats-brought-about-by-globalisation-economics-essay.php?vref=1> [Accessed 23 September 2020].
- UK Essays. 2018b. *Role of SMEs in economic development*. Available from: <https://www.ukessays.com/essays/economics/the-role-of-smes-on-economic-development-economics-essay.php?vref=1> [Accessed 18 October 2020].
- Ukil, A, Jana, D & Sarkar, A De. 2013. A security framework in cloud computing infrastructure. *International Journal of Network Security & its Applications (IJNSA)*. 5(5):11–24.

- Ursachi, G, Horodnic, I & Zait, A. 2015. How Reliable are Measurement Scales? External Factors with Indirect Influence on Reliability Estimators. *Procedia Economics and Finance*. 20(15):679–686. doi.org/10.1016/s2212-5671(15)00123-9.
- Vacca, J. 2017. *Security in the private cloud*. 1st ed. Denver: Taylor and Francis Group, LLC.
- Vasista, TGK. 2015. Strategic business challenges in cloud systems. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*. 5(4):1–3.
- Vatuiu, T, Udrica, M & Tarca, N. 2013. Cloud computing technology - optimal solution for efficient use of business intelligence and enterprise resource planning applications. *Journal of Knowledge Management, Economics and Information Technology*. 2013(1):395–406.
- Venkatesh, V, Brown, SA & Bala, H. 2013. Bridging the qualitative–quantitative divide: Guidelines for conducting mixed methods research in information systems. *Management Information Systems Quarterly*. 37(3):855–879.
- Venkatesh, V, Morris, MG, Davis, GB & Davis, FD. 2018. User acceptance of information technology: Toward a unified view. *MIS Quarterly*. 27(3):425–478.
- Venters, W & Whitley, E. 2012. A critical review of cloud computing: researching desires and realities. *Journal of Information Technology*. 27(3):179-197.
- Ventureburn. 2015. *Study: fewer than half of SA's SMEs use cloud services*. Available from: <http://ventureburn.com/2015/07/cloud-adoption-of-sa-smes-jumps-to-39-this-year/> [Accessed 29 January 2018].
- De Villiers, M. 2012. Models for interpretive Information Systems Research, Part 2: Design research, development research, design-science research and design-based research: A meta-study and examples. In: *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems*. V. Benson & F. Filippaios, Eds. Reading, UK: Academic Conference and Publishing International Limited.
- Vitti, FPA, dos Santos, DR, Westphall, BC, Westphall, CM & Vieira, MMK. 2014. Current issues in cloud computing security and management. In: *TSECURWARE 2014: The Eighth International Conference on Emerging Security Information, Systems and Technologies*. R. Falk & C. Becker, Eds. Lisbon, Portugal. 37–41.

- Vohradsky, D. 2012. Feature cloud risk: 10 principles and a framework for assessment. *ISACA Journal* 5 (2012). 5(2012):1–11.
- Wailgum, T. 2010. *Biggest barriers to business analytics adoption : People, not tech*. Available from: <https://www.networkworld.com/article/2194368/biggest-barriers-to-business-analytics-adoption--people.html> [Accessed 23 January 2020].
- Walczak, M. 2014. *What is cloud business intelligence?* Available from: <https://www.klipfolio.com/resources/articles/what-is-cloud-business-intelligence> [Accessed 12 July 2019].
- Wanjiku, P & Moturi, C. 2016. Cloud computing: transforming medium and high tech industries in Kenya. In: *IST-Africa 2016 Conference Proceedings*. P. Cunningham & M. Cunningham, Eds. IIMC International Information Management Corporation. 1–11.
- Weiner, Y. 2011. *34 Reasons why even small businesses should consider hiring a cybersecurity expert*. Available from: <https://medium.com/thrive-global/34-reasons-why-even-small-businesses-should-consider-hiring-a-cybersecurity-expert-4b9025fb1da9> [Accessed 24 November 2019].
- Wen, H & Sylla, C. 1999. Road map for the evaluation of information technology investment. In: *Measuring Information Technology Investment Payoff: Contemporary Approaches*. in M. and Szewczak, Ed. Addison Wesley, New York: Idea Group Publishing. 142–150.
- Werff, L Van Der, Fox, G, Masevic, I, Emeakaroha, VC, Morrison, JP & Lynn, T. 2019. Building consumer trust in the cloud : an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing: Advances, Systems and Applications*. 8(6):2–17. doi.org/10.1186/s13677-019-0129-8.
- Widyastuti, D & Irwansyah, I. 2018. Benefits and challenges of cloud computing technology adoption in small and medium enterprises (SMEs). *Advances in Economics, Business and Management Research (AEBMR)*. 41:241–246.
- Wild, J. 2018. *Five most common security frameworks explained*. Available from: <https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/> [Accessed 15 August 2020].
- Willcocks, L. 1992. Evaluating information technology investments: Research findings and

- reappraisal. *Journal of Information Systems*. 2(1 992):243–268. doi.org/10.1111/j.1365-2575.1992.tb00081.x.
- Williams, S & French, D. 2014. Theory of planned behaviour variables and objective walking behaviour does not show seasonal variation in a randomised controlled trial. *BMC Public Health*. 14(1):0–10. doi.org/10.1186/1471-2458-14-120.
- Winkler, V (J. R. 2011. Evaluating cloud security: An information security framework. In: *Cloud Computer Security Techniques and Tactics*. 1st ed. A. Ward, Ed. Waltham: ElsevierInc. 233–252. doi.org/10.1016/B978-1-59749-592-9.00009-9.
- Wisdom, J, Suite, E & Horwitz, S. 2014. Innovation adoption: A review of theories and constructs. *Administration Policy in Mental Health*. 41(4):480–502. doi.org/doi:10.1007/s10488-013-0486-4.
- Wise, L. 2016. *Evaluating business intelligence in the cloud*. Available from: <http://www.cio.com/article/3041639/business-intelligence/evaluating-business-intelligence-in-the-cloud.html> [Accessed 12 August 2017].
- Woodhead, J. 2018. *BI Security: Is your business data safe in the Cloud?* Available from: <https://www.fruitionit.co.uk/2018/10/bi-security-is-your-business-data-safe-in-the-cloud/> [Accessed 7 March 2020].
- Woods, J. 2016. *Twilight of the knowledge economy and the rise of digital economy*. Available from: <https://news.sap.com/2016/05/twilight-of-the-knowledge-economy-and-the-rise-of-digital-economy/> [Accessed 17 February 2019].
- Worku, Z. 2013. Analysis of factors that affect the long-term survival of small businesses in Pretoria, South Africa. *Journal of Data Analysis and Information Processing*, 2013. 1(2013):67–84. doi.org/http://dx.doi.org/10.4236/jdaip.2013.14008.
- World Economic and Social Survey. 2018. *Frontier technologies for sustainable development and adoption*. New York. Available from: [https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESS2018\\_es\\_en.pdf](https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESS2018_es_en.pdf) [Accessed 15 March 2020].
- Worster, WT. 2014. The inductive and deductive methods in customary international law analysis: traditional and modern approaches. *Georgetown Journal of International Law*. 3(2):445–521.

- Wu, PF. 2012. A Mixed-Methods Approach for Technology Acceptance Research. *Journal of the Association for Information Systems*. 13(3):172–187.
- Wu, E & Gusman, J. 2019. *Business intelligence in the Cloud*. Available from: <https://altis.com.au/business-intelligence-in-the-cloud/> [Accessed 7 March 2020].
- Yan, Z, Ding, W, Yu, X, Zhu, H & Deng, R. 2016. Deduplication on Encrypted Big Data in Cloud. *IEEE Transactions on Big Data*. 2(2):138–150. doi.org/138–150. doi:10.1109/tbdata.2016.2587659.
- Yauri, BA & Abah, J. 2016. Mitigating security threats in virtualized environments. *IJCSNS International Journal of Computer Science and Network Security*. 16(1):101–108.
- Yin, R. 2012. *Case study research: Applications, design and methods*. 3rd ed. London, Los Angeles, New Delhi, Singapore, Washington DC: SAGE Publications Ltd.
- Youssef, A & Alageel, M. 2012. A framework for secure cloud computing. *International Journal of Computer Science*. 9(4):487–500.
- Yu, Y, Li, M, Hao, J, Li, X & Zhao, L. 2017. Mediating role of trust brief in SMEs’ strategic choice of cloud service. In: *Proceedings of the twenty-third Americas conference on information systems*. 10–12.
- Yusoff, MSB. 2019. ABC of content validation and content validity index calculation. *Education in Medicine Journal*. 11(2):49–54. doi.org/10.21315/eimj2019.11.2.6.
- Zalaghi, H & Khazaei, H. 2016. The role of deductive and inductive reasoning in accounting research and standard setting. *Asian Journal of Finance & Accounting*. 8(121–141). doi.org/DOI: 10.5772/60429.
- Zefeiti, AMB & Mohamad, NA. 2015. Methodological considerations in studying transformational leadership and its outcomes. *International Journal of Engineering Business Management*. 7(10). doi.org/10.5772/60429.
- Zembylas, M & Vrasidas, C. 2005. Globalization, information and communication technologies, and the prospect of a “global village”: Promises of inclusion or electronic colonization? *Journal of Curriculum Studies*. 37(1):65–83. doi.org/10.1080/0022027032000190687.
- Zielinski, D. 2009. Be clear on cloud computing contracts. 54(11):63-65.



- Ziglari, H & Negini, A. 2017. Evaluating cloud deployment models based on security in the EHR system. In: *In 2017 International Conference on Engineering and Technology (ICET)*. Antalya, Turkey: IEEE. 1–6.
- Zineddine, M. 2015. Vulnerabilities and mitigation techniques tuning in the cloud a cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Levy flights. *Computers and Security*. 48(5):1–18. doi.org/10.1016/j.cose.2014.09.002.
- Zunnurhain, K & Vrbsky, S V. 2010. Security attacks and solutions in clouds. *2nd IEEE international conference on cloud computing technology and science*. 145–156. doi.org/doi: 10.5772/60429.

## APPENDICES

### Appendix A: UNISA Ethical clearance

Dear Mr. Moses Moyo (46351574)



Date: 2016-02-16

Application number:  
014/MM/2016/CSET\_SOC

**REQUEST FOR ETHICAL CLEARANCE:** (Towards a security framework for evaluating web and cloud-based business intelligence applications by small and medium sized enterprises)

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your research study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CRIC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:

[http://www.unisa.ac.za/contents/departments/res\\_policies/docs/ResearchEthicsPolicy\\_apprvCounc\\_21Sept07.pdf](http://www.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf)

Please note that the ethical clearance is granted for the duration of this project and if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

A handwritten signature in black ink, appearing to read "EM", is written over a horizontal line.

Prof Ernest Mnkandla  
Chair, College of Science, Engineering and Technology Ethics Sub-Committee

A handwritten signature in black ink, appearing to read "IGG Moche", is written over a horizontal line.

A handwritten signature in black ink, appearing to read "IGG Moche", is written over a horizontal line.

Prof IGG Moche  
Executive Dean, College of Science, Engineering and Technology

RECEIVED

2016-02-24

OFFICE OF THE EXECUTIVE DEAN  
College of Science, Engineering  
and Technology

University of South Africa  
College of Science, Engineering and Technology  
The Science Campus  
C/o Christiaan de Wet Road and Pioneer Avenue,  
Florida Park, Roodepoort  
Private Bag X6, Florida, 1710  
[www.unisa.ac.za/cset](http://www.unisa.ac.za/cset)

The logo for UNISA (University of South Africa) is displayed in a large, bold, sans-serif font. To its right is the logo for the College of Science, Engineering and Technology, which features a stylized wave graphic above the text "college of science, engineering and technology".

## Appendix B: UNISA amended ethics clearance



### UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) ETHICS REVIEW COMMITTEE

16 February 2016  
Updated 26 June 2020

ERC Reference #: 014/MM/2016/CSET\_SOC  
Name: Mr Moses Moyo  
Student #: 46351574  
Staff #:

Dear Mr Moyo

**Decision: Ethics Approval from  
26 June 2020 to 25 June 2025  
(Humans involved)**

**Researcher(s):** Mr Moses Moyo  
46351574@mylife.unisa.ac.za, 078 554 9610, 078 868 4485

**Supervisor (s):** Prof Marianne Look  
lookm@unisa.ac.za, 011 670 9120

**Working title of research:**

**Towards a security framework for evaluating web and cloud based business intelligence applications by small and medium sized enterprises**

**Qualification:** PhD in Information Systems

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Ethics Review Committee for the above mentioned research. Ethics approval is granted for 5 years.

*The **low risk application** was expedited by the College of Science, Engineering and Technology's (CSET) Ethics Review Committee on 26 June 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa COVID-19 position statement on research ethics



University of South Africa  
Pretorius Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA, 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
www.unisa.ac.za

attached.

2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Science, Engineering and Technology's (CSET) Ethics Review Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date 25 June 2025. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

*Note*

*The reference number 014/MM/2016/CSET\_SOC should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.*

Yours sincerely,



---

Mr C Pilkington  
Chair of School of Computing Ethics Review Subcommittee  
College of Science, Engineering and Technology (CSET)  
E-mail: pilkid@unisa.ac.za  
Tel: (011) 471-2130



---

Prof. E Mnkandla  
Director: School of Computing  
College of Science Engineering and  
Technology (CSET)  
E-mail: [mnkane@unisa.ac.za](mailto:mnkane@unisa.ac.za)  
Tel: (011) 670 9104



---

Prof. B Mamba  
Executive Dean  
College of Science Engineering and  
Technology (CSET)  
E-mail: [mambabb@unisa.ac.za](mailto:mambabb@unisa.ac.za)  
Tel: (011) 670 9230



University of South Africa  
Preller Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA, 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)

## Appendix C: Turnitin Digital Receipt



### Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author: **Moses M Moyo**  
Assignment title: **Revision 2**  
Submission title: **Towards a cloud business intelligence security evaluation fr...**  
File name: **amework\_for\_small\_and\_medium\_enterprises\_21\_September...**  
File size: **2.44M**  
Page count: **359**  
Word count: **116,834**  
Character count: **658,720**  
Submission date: **21-Sep-2021 10:39PM (UTC+0200)**  
Submission ID: **1654142052**



Appendix D: Proofreading and editing certificate



*Certificate of Editing*

This is to certify that the dissertation

TOWARDS A CLOUD BUSINESS INTELLIGENCE  
SECURITY EVALUATION FRAMEWORK FOR  
SMALL AND MEDIUM ENTERPRISES

by

MOSES MOYO

has been proofread and edited for English language  
usage.

Date: 10 August 2021

*LHugo*

Lianne Hugo

Language Practitioner  
B.A. (HMS)  
PGCE

## Appendix E: Informed consent form and semi-structured interview schedule

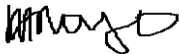
**Dear Participant**

**Unstructured interview schedule to gather data on the evaluation of cloud business intelligence by owners and managers of small and medium enterprises in selected towns in Limpopo Province.**

I am Moses Moyo, a PhD student at UNISA, studying Information, specialising in cloud business intelligence systems security in small and medium enterprises (SMEs) in Limpopo, Province, South Africa. I am inviting you to participate in this study as an interviewee. Upon getting your consent, ... will ask you questions in an interview, either face-to-face or telephonically. The purpose of the interview is to gather general information about the effort you have made in adopting cloud business intelligence, the challenges you faced, how you evaluate the technology. Your views, beliefs, perceptions and knowledge and skills in cloud computing technologies and their adoption are very important in this study. Face-to-face interviews will be conducted at the places and times of your convenience. I seek permission to audio record the interview session so that I will be able to refer to the source during transcription and data analysis. Recordings can always be stopped and/or erased at your request.

It is within your rights to withdraw from (the study) answering the interview when you feel so. There are no correct answers to the questions I will ask you. You are free to give as much information you think will assist in this study. The questions to be asked will not require you to reveal confidential information about your organisations. There are no risks, liabilities or benefits associated with participating in interview sessions. I am assuring you that all responses will remain confidential as regulated by the Ethical policy of UNISA. Do not write your name or company name on this questionnaire as your identity should remain confidential. Show your consent by appending your signature in the spaces below. You may contact the researcher at 0785549610 or [mosesm50@gmail.com](mailto:mosesm50@gmail.com), or my supervisor Professor M Loock, at [loockm@unisa.ac.za](mailto:loockm@unisa.ac.za). Your assistance is greatly appreciated.

**Thank you.**



\_\_\_\_\_  
**Moses Moyo**



**Informed consent statement:**

I have read and understood the purpose of the study as outlined in the letter and that I will NOT be rewarded in any form by participating in the interview. I am voluntarily participating in the interview and consent that the information given is to my best knowledge of security evaluation in cloud-based systems. I am permitting you to use the information in your study and research papers for publication purposes.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Preliminary interview questions**

1. Greeting and welcome of the interviewee
2. Telling the interview, the purpose of the interview and asking for reading and signing of informed consent forms
3. Makes the interviewee feel comfortable
4. The interviewer asks for permission to record the session
5. Briefly tell me about yourself and your business history

| Research question No. | Interview questions  |
|-----------------------|--|
| SRQ1                  | 1.a. Can you describe the effort you made/make as a decision-maker in the adoption and use of Cloud BI or any cloud service by your enterprise?                                    |
|                       | 1b. What challenges do you think to prevent your enterprises from adopting and using Cloud BI (or any other cloud services used in data management)?                               |
|                       | 1c. Briefly describe how these challenges have affected your efforts in assisting your enterprise in adopting and using Cloud BI?  |
| SRQ2                  | 2.a. Briefly describe how you evaluated (or would evaluate) Cloud BI you have adopted or intend to adopt?  |
|                       | 2.b. What security considerations do you make when evaluating Cloud BI for adoption by your enterprise?  |
| SRQ3                  | 3.a. Why do you think it is important for SME owners and managers who use ITs to understand security evaluation in Cloud BI?   |
|                       | 3.b. How does your understanding of security evaluation affect the adoption of Cloud BI by your enterprise?  |
| SRQ4                  | 4a. From your understanding of security evaluation and Cloud BI, what would you consider to be the components of a security framework for evaluating Cloud BI for your enterprise? |

**4.b.** What do you think a security framework should perform to meet the needs of SMEs?

**4.c.** What type of security framework would be suitable for use by SMEs in evaluating Cloud BI?

Do you have any information or anything you want to add to this study?

## Appendix F: Informed Consent and Questionnaire for QUAN phase

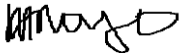
Dear Respondents

### Questionnaire to gather data on security evaluation challenges in cloud-based BI

I am Moses Moyo, a PhD student at UNISA, studying Information, specialising in cloud-based business intelligence systems security in small and medium enterprises (SMEs) in Limpopo, Province, South Africa. I am requesting you to complete this questionnaire which seeks general information about security evaluation knowledge and challenges that SMEs face when intending to adopt cloud business intelligence and related services. Please answer questions using your best knowledge about the security issues in the cloud and your experience. The information you provide will be used to propose a security framework for evaluating cloud-based business intelligence systems.

It is within your rights to withdraw from (the study) answering the questionnaire when you feel so. This questionnaire does not contain any offensive material. There are no risks, liabilities or benefits associated with answering this questionnaire. I am assuring you that all responses will remain confidential as regulated by the Ethical policy of UNISA. Do not write your name or company name on this questionnaire as your identity should remain confidential. Show your consent by appending your signature in the spaces below. You may contact the researcher at 0785549610 or [mosesm50@gmail.com](mailto:mosesm50@gmail.com), or my supervisor Professor M Loock, at [loockm@unisa.ac.za](mailto:loockm@unisa.ac.za). Your assistance is greatly appreciated.

Thank you.



\_\_\_\_\_  
Moses Moyo

### Informed consent statement:

I have read and understood the purpose of the study as outlined in the letter and that I will NOT be rewarded in any form by completing this questionnaire. I am voluntarily completing this questionnaire and consent that the information given is to my best knowledge of security evaluation in cloud-based systems. I am permitting you to use the information in your study and research papers for publication purposes.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**SECTION 1: SMEs DEMOGRAPHIC INFORMATION AND DECISION-MAKERS**

- 1.1. Location of the company \_\_\_\_\_
- 1.2. Product/service category \_\_\_\_\_
- 1.3. Number of employees \_\_\_\_\_
- 1.4. Business type Small Enterprise  Medium Enterprise
- 1.5. a The person in charge of operations The owner  Manager
- 1.5. b. Gender Female  Male
- 1.6. Age range of owner/manager in years 

|         |        |         |         |         |          |
|---------|--------|---------|---------|---------|----------|
| 25 – 30 | 31- 35 | 36 - 40 | 41 - 45 | 46 - 50 | Above 50 |
|---------|--------|---------|---------|---------|----------|
- 1.7. Highest educational qualification Matric  Diploma  BA/BSC  Postgrad
- 1.8. State of IT system used in your enterprise Bad  Fairly good  Good
- 1.9. Type of enterprise data put on the cloud Sensitive  Non-sensitive  Both

**SECTION 2: KNOWLEDGE ABOUT FACTORS INFLUENCING THE ADOPTION AND USE OF CLOUD BI BY SMES IN LIMPOPO PROVINCE**

*Section 2.1 Knowledge about benefits adoption and use of Cloud BI by SMEs in Limpopo Province*

- 2.1.1. Rate your knowledge of Cloud BI Very good  Good  Bad  Very Bad
- 2.1.2. How long you have been aware of Cloud BI < 1 yr.  1 – 3 yrs.  4 – 6 yrs.  > 6 yrs.
- 2.1.3. Your knowledge about the benefits of Cloud BI in SMEs Very good  Good  Bad  Very Bad
- 2.1.4. Indicated the stage of adoption of Cloud BI by your enterprise Awareness  Interest  Evaluation  Testing  Commitment
- 2.1.5. Which stage of technology adoption do you consider to be the most difficult? (Choose one) Awareness  Interest  Evaluation  Testing  Commitment
- 2.1.6. How did you come to know about Cloud BI? Friends  research on the web  e-mail from CSPs  employee
- 2.1.7. How did (do) you choose the cloud BI, or you are currently using or intend to use? Recommended by experts  Research from the web  Friend
- 2.1.8. Types of cloud deployment preferred Public  Community  Private  Hybrid
- 2.1.9. How do you prefer to access Cloud BI? (Choose one) Web  Internet  Both
- 2.1.10. How would you describe your enterprise innovation adoption styles Innovators Early Adopters Early Majority Late Majority Laggards.

**2.1.11. To what extent will each of these benefits of Cloud BI likely to influence you to recommend your enterprise to adopt the technology**

- |  | More likely              | Not sure                 | Less likely              |
|--|--------------------------|--------------------------|--------------------------|
| a. Security of the cloud                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Affordability of service                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. The elasticity of Cloud BI                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Rapid deployment and implementation of Cloud BI | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. On-demand availability of Cloud BI              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| f. The simplicity of Cloud BI                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

|   |  |                          |                          |                          |
|---|--|--------------------------|--------------------------|--------------------------|
| g | Reduced overheads of Cloud BI              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| h | Easy integration with existing technology  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| i | Data analysis, visualisation and reporting | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| j | Improving data management                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| k | Improving decision making                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| l | Improving competitiveness                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| m | Professionalism in information analysis    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| n | Improving customer care                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

## Section 2.2: Knowledge about factors preventing the adoption and use of Cloud BI by SMEs

To what extent do you think that your enterprise is prevented from adopting and using Cloud BI by each of these challenges? (*Very much affected = 4, Moderately impacted = 3, Little impact = 2, No impact = 1*)

|               |  | 4                        | 3                        | 2                        | 1                        |
|---------------|--|--------------------------|--------------------------|--------------------------|--------------------------|
| <b>2.2.1.</b> | <b>Information and data security breaches by cybercriminals and vulnerabilities in the cloud technologies</b>  |                          |                          |                          |                          |
| a.            | Hacking activities breaching data confidentiality  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b.            | Information and data leakage and theft in SaaS   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c.            | Data privacy breaches  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d.            | Sharing of the same data storage with competitors  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e.            | Data and application interoperability and portability  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.2.2.</b> | <b>Mistrust of CSP towards promised services and contracts, data theft and closure of CSP</b>                  |                          |                          |                          |                          |
| a.            | Loss of control of data to providers in the cloud  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b.            | Possibility of CSP closing down without notice   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c.            | Difficulties in data migration to other providers  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d.            | Mistrust of CSPs in keeping enterprise data safe   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e.            | Mistrust of CSPs in adhering to contracts  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.2.3.</b> | <b>Financial risks due to litigation or stalled operations, data availability and corruptions in the cloud</b> |                          |                          |                          |                          |
| a.            | Fear of financial risks due to ransomware  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b.            | Fear of financial risks due to litigation  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c.            | Fear of financial risks due to loss of business  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d.            | Financial risks to hidden subscription fees  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.2.4.</b> | <b>Knowledge and skills challenges related to Cloud BI technologies</b>  |                          |                          |                          |                          |
| a.            | Lack of knowledge about features of Cloud BI   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b.            | Lack of skills in using cloud business intelligence for business purposes                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c.            | Lack of skills to identify and select the most appropriate cloud business intelligence                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d.            | Lack of knowledge about security vulnerabilities in the cloud business intelligence                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e.            | Lack of knowledge of security in different cloud deployment  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

- |    |   |                          |                          |                          |                          |
|----|---|--------------------------|--------------------------|--------------------------|--------------------------|
| f. | Lack of knowledge of the reliability of cloud service providers | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| g. | Lack of knowledge on how the cloud works                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**SECTION 3: KNOWLEDGE OF SECURITY EVALUATION OF CLOUD BI BY DECISION-MAKERS**

**3.1. Importance of understanding of security evaluation of Cloud BI by decision-makers** (5 = strongly agree, 4 = agree, 3 = neutral/not sure, 2 = disagree, and 1 = strongly disagree)

- |    | 5   | 4 | 3 | 2 | 1 |
|----|---|---|---|---|---|
| a. | A good understanding of security evaluation makes decision-makers accountable and responsible for security issues in the enterprise |   |   |   |   |
| b. | A good understanding of security evaluation is important for decision making to be based on evidence and experiences                |   |   |   |   |
| c. | Good knowledge and skills in software evaluation by decision-makers improves security assessment in SMEs                            |   |   |   |   |
| d. | Only decision-makers with good knowledge and skills in Cloud BI evaluation can recommend the adoption of technology                 |   |   |   |   |
| e. | I can only recommend the adoption of Cloud BI when I am very knowledgeable with security evaluation of the technology               |   |   |   |   |
| f. | Only experts in security can evaluate Cloud BI and recommend their adoption   |   |   |   |   |
| g. | Decision-makers in SMEs cannot be held responsible for breach of security of the data they store in the cloud                       |   |   |   |   |
| h. | SMEs are only responsible for data security in a private cloud  |   |   |   |   |

**3.2. Effect of poor understanding of security evaluation on adoption of CLOUD BI in SMEs** (5 = strongly agree, 4 = agree, 3 = neutral/not sure, 2 = disagree, and 1 = strongly disagree)

- |    | 5   | 4 | 3 | 2 | 1 |
|----|---|---|---|---|---|
| a. | Poor understanding of security evaluation of Cloud BI leads to the selection of inappropriate technology solution |   |   |   |   |
| b. | Poor understanding of security evaluation of Cloud BI leads to the reluctance of SMEs adopting and using it.      |   |   |   |   |

**SECTION 4: IMPLEMENTATION OF THE SECURITY EVALUATION PROCESS BY DECISION-MAKERS**

**4.1. To what extent do you agree or disagree with each of these statements with regards to your knowledge about the process of security evaluation of Cloud BI by decision-makers in SMEs (5 = strongly agree, 4 = agree, 3 = neutral/not sure, 2 = disagree, and 1 = strongly disagree)**

|   |                          | <b>Ratings on security evaluation understanding</b> |                          |                          |                          |  |
|---|--------------------------|---|--------------------------|--------------------------|--------------------------|--|
| <b>Statement</b>  | <b>5</b>                 | <b>4</b>  | <b>3</b>                 | <b>2</b>                 | <b>1</b>                 |  |
| <b>a.</b> Checking information asset accessibility publicly by unauthorised cloud users                                 | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>b.</b> Checking the chances of being tricked into signing a contract with a poor performing CSPs                     | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>c.</b> Checking that expected functionalities and results of Cloud BI match claims made by CSPs                      | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>d.</b> Checking whether CSP employees can access and manipulate enterprise data without permission                   | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>e.</b> Checking the level of control of data in the cloud I will have  | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>f.</b> Identifying and understanding exposure to risk and capability of managing it.                                 | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>g.</b> Checking reported cases on whether unexpected changes to data/information in a cloud once occurred            | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>h.</b> Checking whether processes or function on clouds can be manipulated by outsiders                              | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>i.</b> Identifying the possible sources of conflict with the CSP in terms of SLAs                                    | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>j.</b> Checking reports periodically when the cloud was unavailable to the users                                     | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>k.</b> Verifying that the enterprise will be able to migrate its data to another cloud easily                        | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>l.</b> Checking if financial risks are likely to result from hidden subscription costs                               | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>m.</b> Checking if financial risks are likely to result from litigation costs by customers after exposure of data    | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>n.</b> Using security reliability information from various security organisations or publications about the Cloud BI | <input type="checkbox"/> | <input type="checkbox"/>                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |

#### 4.2. Decision-makers' considerations when evaluating Cloud BI

How important do you consider each of these security issues when evaluating cloud-based BI? (Very important =4 Important = 3, Less important =2, Not important =1)

|   | 4                        | 3                        | 2                        | 1                        |
|---|--------------------------|--------------------------|--------------------------|--------------------------|
| a. Data security,                                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Cloud interoperability                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Application and data portability                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Application security                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Backup data and recovery of app                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| f. Firewalls configurations                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| g. Password protection                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| h. Security features of application interfaces        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| i. Compliance with national/international legislation | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| j. Legal and administrative issues                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| k. Responsibilities and liabilities of the enterprise | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| l. Human resources security                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| m. Organizational security and risk management        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| n. Physical security of the provider                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| o. Security guideline by the provider                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| p. Vendor or provider reliability                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

#### SECTION 4.3 CHALLENGES OF SECURITY EVALUATION OF CLOUD BI BY DECISION-MAKERS

To what extent do you think each of the factors is a challenge to the evaluation of cloud-based BI by decision-makers in SMEs. (Very serious = 4, Serious = 3, Less serious =2, Not serious = 1)

|  | 4                        | 3                        | 2                        | 1                        |
|--|--------------------------|--------------------------|--------------------------|--------------------------|
| a. Physical security evaluation of provider                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Evaluating vulnerabilities in the cloud                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Evaluating vulnerabilities in the interface of applications             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. The ability of the provider to meet requirements                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. The security that cloud providers claim they give                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| f. Lack of tools to evaluate Cloud BI                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| g. Authentication of users/applications/ processes,                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| h. Robustness of separation between data belonging to different customers, | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| i. Cloud legal and regulatory issues,                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| j. Incident response before the adoption of cloud-based services           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| k. Getting information from cloud s\providers                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| l. Knowing the physical location of the cloud provider                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| m. Service lease agreements (SLAs)   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| n. Whom you share the cloud with   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| o. Certainty about the survival of cloud provider                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| p. History of data breaches in a cloud                                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| q. Trust of provider and employees   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| r. Lack of knowledge and skills to evaluate CLOUD BI by decision-makers    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |



**SECTION 5: COMPONENTS OF SECURITY EVALUATION FRAMEWORK FOR CLOUD BI**

**5.1. How frequent do you each of these tools and methodologies when evaluating Cloud BI or any cloud-based services you intend to adopt (Always = 4, Sometimes = 3, Rarely = 2 and Never = 1)**

|               | 4                        | 3                        | 2                        | 1                        |
|---------------|--------------------------|--------------------------|--------------------------|--------------------------|
| a. Guidelines | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Checklists | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Standards  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Policies   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Procedure  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| f. Models     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| g. Frameworks | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**5.2. How important do you think each of these could be as a component of a security framework for evaluating Cloud BI by SMEs (Very Important =4, Important = 3, Not sure = 2 and Not Important = 1)**

|               | 4                        | 3                        | 2                        | 1                        |
|---------------|--------------------------|--------------------------|--------------------------|--------------------------|
| a. Guidelines | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Checklist  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Policies   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Procedures | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Models     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**5.3. Based on your knowledge of the uses of the security framework, rate the appropriateness of each of these uses. (Appropriate = 3, not sure = 2 and inappropriate = 1)**

|   | 3                        | 2                        | 1                        |
|---|--------------------------|--------------------------|--------------------------|
| a. Explains to all parties (internal, tangential and external) how information, systems and services are managed within the enterprise            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. To reduce risk levels and the organization’s exposure to vulnerabilities   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Instils confidence in an industry or establish a strong reputation with potential business partners and customers                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Provides a common language and systematic methodology for managing cybersecurity risk  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Provides an enterprise with a chance to identify areas where existing processes may be strengthened, or where new processes can be implemented | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**5.4. Knowledge about the type of framework decision-makers envisaged**

|  | 4                        | 3                        | 2                        | 1                        |
|--|--------------------------|--------------------------|--------------------------|--------------------------|
| Easy to use                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Easy to learn                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Provides simple guidelines on what to do | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| User-friendly                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

*Add any information you may think it is vital to this study:*

---

Thank you for completing this questionnaire

## Appendix G: Informed Consent and Questionnaires for security framework validation

### UNIVERSITY OF SOUTH AFRICA

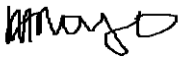
Dear Respondents

**Questionnaire to gather data on the validation of the security evaluation framework for cloud business intelligence for use by small and medium enterprises**

I am Moses Moyo, a PhD student at the University of South Africa (UNISA), studying Information, specialising in cloud-based business intelligence systems security in small and medium enterprises (SMEs) in Limpopo, Province, South Africa. I am requesting you to review the security evaluation framework and checklists provided and then complete the relevance and acceptable validation questionnaires. Please answer questions using your best knowledge about the relevance and acceptability of the security framework concerning its use in SMEs. The information you provide will be used to validate the new security framework.

It is within your rights to withdraw from (the study) answering the questionnaire when you feel so. This questionnaire does not contain any offensive material. There are no risks, liabilities or benefits associated with answering this questionnaire and participating in the study. I am assuring you that all responses will remain confidential as regulated by the Ethical policy of UNISA. Do not write your name or company name on this questionnaire as your identity must remain confidential. Show your consent by appending your signature in the spaces below. You may contact the researcher at 0785549610 or [mosesm50@gmail.com](mailto:mosesm50@gmail.com), [46351574@mylife.unisa.ac.za](mailto:46351574@mylife.unisa.ac.za) or my supervisor Professor M Loock, at [loockm@unisa.ac.za](mailto:loockm@unisa.ac.za). Your assistance is greatly appreciated.

Thank you.

\_\_\_\_\_  \_\_\_\_\_

Date: 21 May 2020

Moses Moyo

**Informed consent statement:**

I have read and understood the purpose of the study as outlined in the letter and that I will NOT be rewarded in any form by completing this questionnaire. I am voluntarily completing this questionnaire and consent that the information given is to my best knowledge of the security evaluation framework provided. I am permitting you to use the information in your study and research papers for publication purposes.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**This questionnaire consists of three sections:**  
SECTION 1: DEMOGRAPHIC INFORMATION  
SECTION 2: CONTENT VALIDATION  
SECTION 3: FACE VALIDATION

**SECTION A: DEMOGRAPHIC INFORMATION**

**Please complete this section by placing a tick  $\checkmark$  or cross x in the spaces provided**

**Gender:**

- Female
- Male
- Other

**Age group:**

- Below 20
- 20 to 30
- 31 to 40
- 41 to 50
- Above 50

**Highest educational qualification:**

- Matric
- Diploma
- Bachelor's degree
- Honours degree
- Doctorate

**Occupation:**

- IT specialist
- Security specialist
- Database Admin
- SME owner
- SME Manager

**Duration in your occupation (years):**

- Less than 2 years
- 2 to 5 years
- 5 to 10 years
- more than 10 years

## Section 2: Relevance validation of security evaluation framework

| Validation of relevance of a security evaluation framework for cloud business intelligence for use by SMEs  |           |          |          |          |
|---|-----------|----------|----------|----------|
| <b>Dear Experts</b>   |           |          |          |          |
| This section of the questionnaire contains 7 components and 37 items related to the security evaluation framework for cloud business intelligence solutions and its checklists you are provided with. We need your <i>expert</i> judgement on the degree of the <b>relevance</b> of each item to measure the suitability of each component of the framework. Your review should be based on the definition and relevant components, terminology, and activities that are provided to you. Please be as objective and constructive as possible in your review and use the following rating scale |           |          |          |          |
| <b>Degree of relevance or acceptance</b>  |           |          |          |          |
| 1= the item is not relevant to the security evaluation component  |           |          |          |          |
| 2 = the item is relevant to the security evaluation component   |           |          |          |          |
| 3 = the item is quite relevant to the security evaluation component   |           |          |          |          |
| 4 = the item is highly relevant to the security evaluation component  |           |          |          |          |
| <hr/>   |           |          |          |          |
| Items   | Relevance |          |          |          |
| <b>1. Assessing business needs and data security needs</b>  | <b>1</b>  | <b>2</b> | <b>3</b> | <b>4</b> |
| 1.1. Assess alignment of data management plans to business needs  |           |          |          |          |
| 1.2. Classification of data to be migrated, stored and managed in the cloud on their sensitivity or security needs  |           |          |          |          |
| 1.3. Assessing security requirements of data to be migrated to the cloud  |           |          |          |          |
| <hr/>   |           |          |          |          |
| <b>2. Cloud business intelligence usability assessment</b>  | <b>1</b>  | <b>2</b> | <b>3</b> | <b>4</b> |
| 2.1. Assess the functionalities of CLOUD BI on key data management and security   |           |          |          |          |
| 2.2. Assessing security vulnerabilities, threats and risks in shortlisted CLOUD BI  |           |          |          |          |
| 2.3. Assessing security controls in place and their robustness  |           |          |          |          |
| 2.4. Assessing CLOUD BI usability by non-technical users  |           |          |          |          |
| 2.5. Assessing the knowledge and skills needed to use each service delivery model   |           |          |          |          |
| 2.6. Assessing the cost and financial risks of each shortlisted CLOUD BI solution   |           |          |          |          |
| <hr/>   |           |          |          |          |
| <b>3. Cloud business intelligence service delivery models assessment</b>  | <b>1</b>  | <b>2</b> | <b>3</b> | <b>4</b> |
| 3.1. Assess security vulnerabilities, threats and risks for each service delivery model   |           |          |          |          |
| 3.2. Assessing costs of using each service delivery model   |           |          |          |          |
| 3.4. Assessing financial risks due to security risks in each service delivery model   |           |          |          |          |
| <hr/>   |           |          |          |          |
| <b>4. Cloud deployment models assessment</b>  | <b>1</b>  | <b>2</b> | <b>3</b> | <b>4</b> |
| 4.1 Assess vulnerabilities, threats and risks in each deployment model  |           |          |          |          |
| 4.2. Assessing the effectiveness of security controls in place  |           |          |          |          |
| 4.3. Assessing the availability, reliability and performance of the cloud deployment model  |           |          |          |          |
| 4.4. Assessing cloud interoperability and application portability   |           |          |          |          |
| 4.5 Assessing costs of each deployment model  |           |          |          |          |
| 4.6. Assessing financial risks of using the deployment model:   |           |          |          |          |
| <hr/>   |           |          |          |          |
| <b>5. Assessment of cloud service providers</b>   | <b>1</b>  | <b>2</b> | <b>3</b> | <b>4</b> |
| 5.1. Check CSP technologies and services roadmap  |           |          |          |          |
| 5.2. Assess data governance and security  |           |          |          |          |
| 5.3. Examine certification and standards  |           |          |          |          |
| 5.4. Assess trust, reliability and performance of CSPs  |           |          |          |          |
| 5.5. Assess business healthy and profile of CSP   |           |          |          |          |
| 5.6. Assess business continuity of CSP  |           |          |          |          |

|  |          |          |          |          |
|--|----------|----------|----------|----------|
| 5.7. Assess cloud service agreement and contracts  |          |          |          |          |
| 5.8. Assess service dependence and partnerships  |          |          |          |          |
| 5.9. Assess the availability of information on recent breaches and mitigation strategies                     |          |          |          |          |
| <b>6. Financial risks assessment</b>   |          |          |          |          |
|  | <b>1</b> | <b>2</b> | <b>3</b> | <b>4</b> |
| 6.1. Assessing hidden costs  |          |          |          |          |
| 6.2. Assessing costs due to downtime   |          |          |          |          |
| 6.3. Assessing litigation costs  |          |          |          |          |
| 6.4. Assessing penalty costs for misuse of services  |          |          |          |          |
| <b>7. Addresses traditional security standards and frameworks</b>  |          |          |          |          |
|  | <b>1</b> | <b>2</b> | <b>3</b> | <b>4</b> |
| 7.1. COBIT for IT governance and bringing in the best practices  |          |          |          |          |
| 7.2. ISRM for assessing security risks in assets and manage them   |          |          |          |          |
| 7.3. ISO 27001 for compliance to standards for information security policies and standards and certification |          |          |          |          |
| 7.4. NIST for cybersecurity assessment and management  |          |          |          |          |
| 7.5. ERM for cyber risk management in cloud environments   |          |          |          |          |

### Section 3: Face validation of security evaluation framework

|   |  |          |          |          |
|---|--|----------|----------|----------|
| <b>Acceptance validation of a security evaluation framework for cloud business intelligence for use by SMEs</b>   |  |          |          |          |
| <p>The section of the questionnaire contains 5 sections and <b>30</b> items related to the security evaluation framework and its checklists you are provided with. You are requested to review the framework for its <b>acceptance</b> as a tool for security evaluation in cloud business intelligence by SME decision-makers with basic IT and security skills. Your review should focus on the usefulness and suitability of framework components, suggested activities and checklists. Please be as objective and constructive as possible in your review and use the following rating scale.</p> <p><b>Degree of acceptability of cloud business intelligence security evaluation framework in security evaluation</b><br/> 3 = the item is highly acceptable to the security evaluation component<br/> 2 = the item is acceptable to the security evaluation component<br/> 1 = the item is not acceptable to the security evaluation component</p> |  |          |          |          |
| <b>Items validated</b>  |  |          |          |          |
| <b>Acceptance</b>   |  |          |          |          |
| <b>Acceptability of each component of the security evaluation framework in CLOUD BI</b>   |  | <b>3</b> | <b>2</b> | <b>1</b> |
| 1.1. Assessment of business and data management and security needs  |  |          |          |          |
| 1.2. Assessment of Cloud business intelligence usability and security functionalities   |  |          |          |          |
| 1.3. Assessing security vulnerabilities and threats in service delivery models offered  |  |          |          |          |
| 1.4. Assessing cloud deployment model with which the cloud service is provided  |  |          |          |          |
| 1.5. Assessing cloud services providers' security, trust, reliability and performance   |  |          |          |          |
| 1.6. Assessment of financial risks due to security issues in the cloud and cloud providers  |  |          |          |          |
| <b>2. Validating cloud business intelligence security evaluation framework evaluation activities acceptance</b>   |  |          |          |          |
|   |  | <b>3</b> | <b>2</b> | <b>1</b> |
| 2.1. Scope of security evaluation covered by activities to be performed acceptably  |  |          |          |          |
| 2.2. The link between activities and a respective component of CBISEF   |  |          |          |          |
| 2.3. The provision by each activity in security evaluation of Cloud BI before adoption  |  |          |          |          |
| 2.5. The easiness with which activities can be conducted by persons with limited IT skills  |  |          |          |          |
| 2.6. The sequence of the components and activities in security evaluation   |  |          |          |          |

|   |  |          |          |          |
|---|--|----------|----------|----------|
| <b>3. Validating cloud business intelligence security evaluation framework checklists acceptance</b>                      |  | <b>3</b> | <b>2</b> | <b>1</b> |
| 3.1. Completeness of coverage of assessment activities for each component in checklists                                   |  |          |          |          |
| 3.2. Suitability of items checklist assessing the specified aspects in the evaluation process                             |  |          |          |          |
| 3.3. Checklists can be used to evaluate each aspect of the framework  |  |          |          |          |
| 3.4. The elaborateness of items and ease of use in assessing aspects referred to  |  |          |          |          |
| 3.5. Scoring of each item in each checklist   |  |          |          |          |
| 3.6. The explicitness of summary of evaluation major components   |  |          |          |          |
| 3.7. Clarity of decision-making comparison list   |  |          |          |          |
| 3.8. Weights and criteria for decision making in the decision-making checklist  |  |          |          |          |
| 3.9. The effort needed to use the checklists in evaluating each component   |  |          |          |          |
| <b>4. Validating the acceptance of language used, length and layout of checklists</b>                                     |  | <b>3</b> | <b>2</b> | <b>1</b> |
| 4.1. Appropriateness of language used in the checklists non-IT decision-makers  |  |          |          |          |
| 4.2. Checklist layout makes it easy to identify items to be evaluated   |  |          |          |          |
| 4.3. Number of items to assess the aspects of a components  |  |          |          |          |
| 4.4. The layout of items on checklists allows easy use by an average user   |  |          |          |          |
| <b>5. Validating the acceptance of CBISEF in implementing traditional security standards and frameworks</b>               |  | <b>3</b> | <b>2</b> | <b>1</b> |
| 5.1. Level of using IT and security governance and the best practices (COBIT) framework                                   |  |          |          |          |
| 5.2. Implementing ISRM for security risks manage in enterprise information assets   |  |          |          |          |
| 5.3. Incorporates ISO 27001 for compliance to standards for information security policies and standards and certification |  |          |          |          |
| 5.4. Enabling the use of NIST for cybersecurity assessment and management   |  |          |          |          |
| 5.5. Coverage of ERM for cyber risk management in cloud environments  |  |          |          |          |
| Please write any comments you think may be valuable in the validation of the framework                                    |  |          |          |          |

e-mail the completed questionnaire to *mosesm50@gmail.com*, *46351574@mylife.unisa.ac.za* or *WhatsApp to 0785549610*. Thank you for participating in this study

## Appendix H: Tables referenced in Chapter 3

**Table AP3.1: Mixed methods designs, characteristics, purpose, and suitability**

| Strategy                  | Characteristics   | Purpose   | Emphasis                   |
|---------------------------|---|---|----------------------------|
| Concurrent triangulation  | The design allows the simultaneous collection of both quantitative and qualitative data which the researcher compare to establish similarities, differences, and combinations.  | The use of both methods is intended to offset the shortfalls utilising a single method with the strength of another.      | QUAN & QUAL                |
| Concurrent nested         | Both quantitative and qualitative data are collected at the same time, but one there is one main method that guides the research while the other a secondary method.            | This is useful when addressing different questions from the major one or when information from different levels is needed | Qual (QUAN) → Quan (QUAL)  |
| Concurrent transformative | Both quantitative and qualitative data are collected at the same time to support a specific theoretical perspective, but the researcher incorporates one method into the other. | This is useful when the research study is evaluating a theory at different levels of analysis.                            | QUAN & QUAL → Quan         |
| Sequential explanatory    | The initial stage of the research emphasises quantitative data collection and analysis. Qualitative data collection and analysis followed to support quantitative results.      | Qualitative results are used to substantiate the findings of a quantitative study to explain a phenomenon                 | QUAN → Qual                |
| Sequential exploratory    | Qualitative data is collected and analysed, first, an instrument or theory is developed, then, quantitative data is collected analysed to support the qualitative results.      | Used to explore a social phenomenon. This design is useful when developing and testing a new instrument.                  | QUAL → Quan                |
| Sequential transformative | Involves collecting and analysing qualitative or quantitative data in different stages to verify a theoretical perspective  | Employs the best methods that support a theoretical perspective   | QUAL → Quan<br>QUAN → Qual |

Adapted from Creswell (2013) and Creswell and Plano-Clark (2011) for this study

## Appendix J: Tables referenced in Chapter 4

**Table AP4.1: Reliability of the survey questionnaire items used in the QUAN phase**

| Item  | n = 57           |                  |
|---|------------------|------------------|
|   | No. of variables | Cronbach's Alpha |
| <b>Section 1: SMEs Demographic information and decision-makers</b>  | 8                | 0.687            |
| <b>Section 2.1: Knowledge about the benefits of using Cloud BI</b>  |                  |                  |
| 2.1.1. Knowledge about Cloud BI by decision-makers in Limpopo Province  | 9                | 0.605            |
| 2.1.2. Knowledge about the benefits of the adoption and use of Cloud BI by SMEs   | 14               | 0.683            |
| <b>Section 2.2: Knowledge about factors preventing the adoption and use of Cloud BI by SMEs</b>   |                  |                  |
| 2.2.1. Information and data security breaches by cybercriminals and vulnerabilities in the cloud technologies                                 | 5                | 0.708            |
| 2.2.2. Mistrust of CSP towards promised services and contracts, data theft and closure of CSP   | 5                | 0.755            |
| 2.2.3. Financial risks due to litigation or stalled operations, data availability and corruptions in the cloud                                | 4                | 0.792            |
| 2.2.4. Knowledge and skills challenges  | 7                | 0.701            |
| <b>SECTION 3: Security evaluation of Cloud BI by decision-makers on the</b>   |                  |                  |
| 3.1. Importance of understanding of security evaluation of Cloud BI by decision-makers  | 8                | 0.785            |
| 3.3. Knowledge about the process of security evaluation of Cloud BI by decision-makers  | 14               | 0.859            |
| 3.2. Effect of poor understanding of security evaluation on the adoption of Cloud BI  | 2                | 0.676            |
| <b>Section 4: Challenges of the security evaluation process by decision-makers</b>  |                  |                  |
| 4.3. Perceived challenges of security evaluation of Cloud BI by decision-makers   | 18               | 0.675            |
| 4.2. Decision-makers' perceptions about considerations when evaluating Cloud BI   | 16               | 0.756            |
| <b>Section 5: Knowledge of tools and methodologies used in evaluating security in Cloud BI</b>  |                  |                  |
| 5.1. Frequency of use of security evaluation tools and methodologies when evaluating Cloud BI or any cloud-based services you intend to adopt | 7                | 0.657            |
| 5.2. Important components of a security framework for evaluating Cloud BI by SMEs   | 5                | 0.688            |
| 5.3. Perceptions and beliefs of the uses of the security framework  | 5                | 0.671            |
| Overall questionnaire reliability   | 128              | 0.863            |



**Table AP4.2: Chi-Square test knowledge about and benefits of Cloud BI**

|   |           | Knowledge of the existence of Cloud BI |      |           |       |      |
|---|-----------|--|------|-----------|-------|------|
|   |           | Bad                                    | Good | Very good | Total |      |
| <b>Knowledge about benefits of Cloud BI in SMEs</b> | Bad       | Count                                  | 1    | 3         | 0     | 4    |
|   |           | Expected Count                         | 0.2  | 0.7       | 0.1   | 8.5  |
|   | Good      | Count                                  | 4    | 29        | 2     | 35   |
|   |           | Expected Count                         | 7.4  | 24.6      | 3.1   | 35.0 |
|   | Very good | Count                                  | 0    | 11        | 3     | 14   |
|   |           | Expected Count                         | 2.9  | 9.8       | 1.2   | 14.0 |
|   | Total     | Count                                  | 12   | 40        | 5     | 57   |
|   |           | Expected Count                         | 12.0 | 40.0      | 5.0   | 57.0 |

| Chi-Square Tests             |                     |    |                                   |
|------------------------------|---------------------|----|-----------------------------------|
|                              | Value               | df | Asymptotic Significance (2-sided) |
| Pearson Chi-Square           | 38.360 <sup>a</sup> | 6  | 0.000                             |
| Likelihood Ratio             | 35.809              | 6  | 0.000                             |
| Linear-by-Linear Association | 25.798              | 1  | 0.000                             |
| N of Valid Cases             | 57                  |    |                                   |

a. 9 cells (75.0%) have expected count less than 5. The minimum expected count is .09.

**Table AP4.3: Knowledge of strategies in security evaluation in Cloud BI**

| Activity   | Ratings (n = 57)     |             |                |                |                          | Mean | Std. Dev |
|--|----------------------|-------------|----------------|----------------|--------------------------|------|----------|
|  | Strongly agree f (%) | Agree f (%) | Not sure f (%) | Disagree f (%) | Strongly disagreed f (%) |      |          |
| <b>1. Evaluating data security in the cloud</b>  |                      |             |                |                |                          |      |          |
| Assessing information asset accessibility publicly by unauthorised cloud users                       | 27 (47.3)            | 25 (43.9)   | 5 (8.8)        | 0 (0.0)        | 0 (0.0)                  | 4.4  | 0.6      |
| Checking whether CSP employees can access and manipulate enterprise data without permission          | 21 (36.8)            | 27 (47.4)   | 8 (14)         | 1 (1.8)        | 0 (0.0)                  | 4.2  | 0.7      |
| Verifying that the enterprise will be able to migrate its data to other cloud providers easily       | 26 (45.6)            | 21 (36.8)   | 5 (8.8)        | 4 (7.0)        | 1 (1.8)                  | 4.2  | 1.0      |
| Identifying and understanding exposure to risk and the capability of managing it.                    | 20 (35.1)            | 27 (47.4)   | 6 (10.4)       | 1 (1.8)        | 3 (5.3)                  | 4.1  | 1.0      |
| Checking whether processes or function on clouds can be manipulated by outsiders                     | 22 (38.6)            | 25 (43.8)   | 5 (8.8)        | 4 (7.0)        | 1 (1.8)                  | 4.1  | 1.0      |
| Checking reports on periods of time when the cloud was unavailable to the users                      | 22 (38.6)            | 24 (42.1)   | 3 (5.3)        | 4 (7.0)        | 4 (7.0)                  | 4.0  | 1.2      |
| Checking reported cases of whether unexpected changes to data / information in a cloud once occurred | 17 (29.8)            | 25 (43.9)   | 8 (14.0)       | 2 (3.5)        | 5 (8.8)                  | 3.8  | 1.2      |
| <b>2. Evaluating security functionalities in Cloud BI interfaces</b>                                 |                      |             |                |                |                          |      |          |

| Activity  | Ratings (n = 57)     |             |                |                |                          | Mean | Std. Dev |
|---|----------------------|-------------|----------------|----------------|--------------------------|------|----------|
|   | Strongly agree f (%) | Agree f (%) | Not sure f (%) | Disagree f (%) | Strongly disagreed f (%) |      |          |
| Checking that expected functionalities and results of Cloud BI match claims made by CSPs                              | 20 (35.1)            | 30 (52.6)   | 5 (8.7)        | 1 (1.8)        | 1 (1.8)                  | 4.2  | 0.8      |
| <b>3. Evaluating CSP related issues</b>   |                      |             |                |                |                          |      |          |
| Using security reliability information from various security organisations or publications about the Cloud BI or CSPs | 18 (31.6)            | 26 (45.6)   | 10 (17.5)      | 3 (5.3)        | 0 (0.0)                  | 4.0  | 0.8      |
| Checking the level of control of data in the cloud I will have  | 17 (29.8)            | 25 (43.9)   | 5 (8.8)        | 8 (14.0)       | 2 (3.5)                  | 3.8  | 1.1      |
| <b>4. Evaluating contracts</b>  |                      |             |                |                |                          |      |          |
| Checking the chances of being tricked into signing a contract with a poor performing CSPs                             | 22 (38.6)            | 30 (52.6)   | 4 (7)          | 1 (1.8)        | 0 (0.0)                  | 4.3  | 0.7      |
| Identifying the possible sources of conflict with the CSP in terms of SLAs  | 18 (31.5)            | 28 (49.1)   | 5 (8.8)        | 5 (8.8)        | 1 (1.8)                  | 4.0  | 1.0      |
| <b>5. Evaluating financial risks</b>  |                      |             |                |                |                          |      |          |
| Checking if financial risks are likely to result from hidden subscription costs                                       | 22 (38.6)            | 21 (36.8)   | 7 (12.3)       | 7 (12.3)       | 0 (0.0)                  | 4.0  | 1.0      |
| Checking if financial risks are likely to result from litigation costs by customers after exposure of their data      | 18 (31.6)            | 26 (45.6)   | 7 (12.3)       | 6 (10.5)       | 0 (0.0)                  | 4.0  | 0.9      |

**Table AP4.4: Considerations to be made during security evaluations**

| Considerations made during evaluation of Cloud BI  | Ratings (n = 57)     |                 |                      |                     | Mean | Std. Dev |
|--|----------------------|-----------------|----------------------|---------------------|------|----------|
|  | Very important f (%) | Important f (%) | Less important f (%) | Not important f (%) |      |          |
| Data security issues in the cloud                  | 41 (71.9)            | 15 (26.3)       | 1 (1.8)              | 0 (0)               | 3.7  | 0.5      |
| Application and data portability                   | 40 (70.2)            | 13 (22.7)       | 3 (5.3)              | 1 (1.8)             | 3.6  | 0.7      |
| Cloud interoperability                             | 33 (57.9)            | 22 (38.6)       | 2 (3.5)              | 0 (0)               | 3.5  | 0.6      |
| Application security                               | 30 (52.6)            | 24 (42.1)       | 3 (5.3)              | 0 (0)               | 3.5  | 0.6      |
| Data backup and recovery strategy                  | 22 (38.6)            | 29 (50.9)       | 4 (7.0)              | 2 (3.5)             | 3.2  | 0.7      |
| Firewalls configurations                           | 18 (31.6)            | 30 (52.6)       | 8 (14)               | 1 (1.8)             | 3.1  | 0.7      |
| Password protection                                | 14 (24.6)            | 37 (64.8)       | 3 (5.3)              | 3 (5.3)             | 3.1  | 0.7      |
| Legal and administrative issues                    | 20 (35.1)            | 25 (43.8)       | 9 (15.8)             | 3 (5.3)             | 3.1  | 0.9      |
| Vendor or service provider reliability             | 24 (42.1)            | 23 (40.3)       | 3 (5.3)              | 7 (12.3)            | 3.1  | 1.0      |
| Security features of application interfaces        | 13 (22.8)            | 35 (61.4)       | 5 (8.8)              | 4 (7.0)             | 3.0  | 0.8      |
| Compliance with national/international legislation | 15 (26.3)            | 31 (54.4)       | 7 (12.3)             | 4 (7.0)             | 3.0  | 0.8      |
| Security guideline by provider                     | 20 (35.1)            | 22 (38.6)       | 9 (15.8)             | 6 (10.5)            | 3.0  | 1.0      |
| Responsibilities and liabilities of enterprise     | 18 (31.6)            | 26 (45.6)       | 5 (8.8)              | 8 (14)              | 2.9  | 1.0      |
| Organizational security and risk management        | 17 (29.8)            | 24 (42.1)       | 7 (12.3)             | 9 (15.8)            | 2.9  | 1.0      |
| Physical security of provider                      | 14 (24.6)            | 23 (40.3)       | 13 (22.8)            | 7 (12.3)            | 2.8  | 1.0      |

**Table AP4.5: Chi-Square test dependence on educational level and security evaluation**

| Variables                         |  | Chi-Square          | df | Asymptotic Significance (2-sided) |
|-----------------------------------|--|---------------------|----|-----------------------------------|
| Highest educational qualification | A good understanding of security evaluation makes decision makers accountable and responsible in security issues in the enterprise | 23.288 <sup>a</sup> | 6  | 0.001                             |
|                                   | A good understanding of security evaluation is important for decision making to be based on evidence and experiences               | 29.863 <sup>a</sup> | 8  | 0.000                             |
|                                   | Good knowledge and skills in software evaluation by decision makers improves security assessment in SMEs                           | 13.876 <sup>a</sup> | 6  | 0.031                             |
|                                   | Only decision makers with good knowledge and skills in CBI evaluation can recommend the adoption of technology                     | 22.539 <sup>a</sup> | 8  | 0.004                             |
|                                   | I can only recommend the adoption of CBI when I am well knowledgeable with security evaluation of the technology                   | 18.555 <sup>a</sup> | 6  | 0.005                             |
|                                   | Only experts in security can evaluate CBI and recommend their adoption   | 18.221 <sup>a</sup> | 8  | 0.02                              |
|                                   | Decision makers in SMEs cannot be held responsible for breach of security of the data they store in the cloud                      | 16.218 <sup>a</sup> | 8  | 0.039                             |
|                                   | SMEs are only responsible for data security in a private cloud   | 5.392 <sup>a</sup>  | 8  | 0.041                             |

**Table AP4.6: Challenges of evaluation of Cloud BI among decision-makers**

| Challenges in the evaluation of Cloud BI   | Ratings n = 57        |                  |                       |                      | Mean | Std. Dev |
|--|-----------------------|------------------|-----------------------|----------------------|------|----------|
|  | Very serious<br>f (%) | Serious<br>f (%) | Less serious<br>f (%) | Not serious<br>f (%) |      |          |
| <b>Limited knowledge and skills in evaluating security in cloud business intelligence solutions</b>      |                       |                  |                       |                      |      |          |
| In ability to evaluate the physical security of provider infrastructure                                  | 39 (68.4)             | 13 (22.8)        | 4 (7.0)               | 1 (1.8)              | 3.7  | 0.6      |
| With ability to evaluate vulnerabilities in the cloud where BI will be deployed                          | 36 (63.2)             | 19 (33.3)        | 2 (3.5)               | 0 (0.0)              | 3.6  | 0.6      |
| Evaluating flaws in interface of BI applications   | 31 (54.4)             | 19 (33.3)        | 6 (10.5)              | 1 (1.8)              | 3.4  | 0.8      |
| Lack of skills to use existing evaluation tools  | 29 (50.8)             | 20 (35.1)        | 5 (8.8)               | 3 (5.3)              | 3.3  | 0.8      |
| Assessing financial risks due to liabilities security breaches   | 21 (36.8)             | 22 (38.6)        | 10 (17.5)             | 4 (7.0)              | 3.1  | 0.9      |
| Understanding Service Lease Agreements from providers  | 25 (43.9)             | 18 (31.5)        | 5 (8.8)               | 9 (15.8)             | 3.0  | 1.1      |
| Understating cloud legal and regulatory issues from various regions                                      | 18 (31.6)             | 22 (38.6)        | 10 (17.5)             | 7 (12.3)             | 2.9  | 1.0      |
| <b>Ignorance or lack of tools and methodologies to evaluate the cloud business intelligence solution</b> |                       |                  |                       |                      |      |          |
| Assessing the ability of the provider to meet contractual requirements                                   | 19 (33.3)             | 31 (54.4)        | 3 (5.3)               | 4 (7.0)              | 3.1  | 0.8      |
| Ascertaining the long-term survival of cloud provider  | 21 (36.8)             | 24 (42.1)        | 9 (15.8)              | 3 (5.3)              | 3.1  | 0.9      |
| Ignorance of suitable tools to use in evaluating Cloud BI in the cloud                                   | 13 (22.8)             | 34 (59.6)        | 7 (12.3)              | 3 (5.3)              | 3.0  | 0.8      |
| Assessing reliability of user authentication by BI applications  | 16 (28.1)             | 29 (50.8)        | 9 (15.8)              | 3 (5.3)              | 3.0  | 0.8      |
| Ascertaining the security controls the cloud providers claim they give                                   | 15 (26.3)             | 32 (56.1)        | 7 (12.3)              | 3 (5.3)              | 3.0  | 0.8      |
| Ascertaining the robustness of separation between data belonging to different customers                  | 17 (29.8)             | 21 (36.8)        | 12 (21.1)             | 7 (12.3)             | 2.8  | 1.0      |
| <b>Lack of relevant information to use in evaluating cloud business intelligence solution</b>            |                       |                  |                       |                      |      |          |
| Difficulty in obtaining historical information of data breaches in a cloud                               | 25 (43.9)             | 22 (38.6)        | 6 (10.5)              | 4 (7.0)              | 3.2  | 0.9      |
| Getting relevant information about BI from cloud providers   | 22 (38.6)             | 22 (38.6)        | 9 (15.8)              | 4 (7.0)              | 3.1  | 0.9      |

| <b>Challenges in the evaluation of Cloud BI</b>                      | <b>Ratings n = 57</b> |                |                     |                    | <b>Mean</b> | <b>Std. Dev</b> |
|--|-----------------------|----------------|---------------------|--------------------|-------------|-----------------|
|  | <b>Very serious</b>   | <b>Serious</b> | <b>Less serious</b> | <b>Not serious</b> |             |                 |
|  | <b>f (%)</b>          | <b>f (%)</b>   | <b>f (%)</b>        | <b>f (%)</b>       |             |                 |
| Assessing the level of trust of the provider and employees with data | 23 (40.4)             | 21 (36.8)      | 9 (15.8)            | 4 (7.0)            | 3.1         | 0.9             |
| Assessing the physical security of the cloud provider                | 13 (22.8)             | 29 (50.9)      | 10 (17.5)           | 5 (8.8)            | 2.9         | 0.9             |
| Assessing risks posed by other users with whom the cloud is shared   | 17 (29.8)             | 26 (45.6)      | 8 (14.1)            | 6 (10.5)           | 2.9         | 0.9             |

**Appendix K: Figures referenced in Chapter 6**

| <b>1. ASSESSING BUSINESS NEEDS AND DATA SECURITY REQUIREMENTS IN THE CLOUD</b>   |   |              |  |
|--|---|--------------|--|
| <b>Date of assessment:</b> .....   |   |              |  |
| <b>Instructions:</b> These statements represent a checklist of key characteristics to consider when assessing the alignment of business needs and data security requirements. Please indicate in the score column whether or not the information provided in the statement meets each criterion for each statement ( <i>1 = criterion met; 0 = criterion not met</i> ) |   |              |  |
| <b>Evaluation criteria</b>   | <b>Statement description</b>  | <b>Score</b> |  |
| <b>Alignment of data management systems with business needs</b>  | Most of the enterprise data is in electronic format and processed electronically  |              |  |
|  | Enterprise data is updated regularly  |              |  |
|  | Enterprise data management plans support business plans and needs   |              |  |
|  | The enterprise is already using cloud services for data storage   |              |  |
|  | Storage is a reason to migrate data to the cloud  |              |  |
| <b>Classification data to be migrated to and managed on the cloud regarding sensitivity or security needs</b>  | Sensitive data is (can be) segregated from non-sensitive data   |              |  |
|  | Data is (will be) accessible only to authorised users of the system   |              |  |
|  | I can identify and decide on which data to migrate to the clouds  |              |  |
|  | Data security is a reason for migrating sensitive data to clouds  |              |  |
| <b>Security requirements of data to be migrated to and managed on the cloud</b>  | Enterprise information security program is supported by policies, procedures, standards, regulatory and compliance requirements |              |  |
|  | Data in the cloud will be protected by  | Passwords    |  |
|  |   | Encryption   |  |
|  | In your enterprise, a migration roadmap directs data classification and protection  |              |  |
|  | Enterprise data requires a high level of security to be stored in the cloud   |              |  |
|  | Enterprise data security goals are easy to understand and simple to implement   |              |  |
|  | Only authorised persons will access and manage data in the cloud  |              |  |
| <i>(if % &lt; 85%: align data management processes and security requirements to enterprise business needs)</i>   |   |              |  |
| <b>Expected score</b>  |   | <b>16</b>    |  |
| <b>Actual score</b>  |   |              |  |
| <b>% of Actual score / Expected score</b>  |   |              |  |

**Figure AP6.1: Checklist 1: Assessing business and data security requirements**

| 2. ASSESSING CLOUD BUSINESS INTELLIGENCE USABILITY  |   |           |
|---|---|-----------|
| Name of Cloud BI:..... Date of Assessment:.....   |   |           |
| <b>Instructions:</b> These statements represent a checklist of key characteristics to consider when evaluating cloud business intelligence. Please indicate in the score/answer column whether or not the information provided in the statement meets each criterion for each statement ( <i>1 = criterion met; 0 = criterion not met</i> ) |   |           |
| Evaluation criteria   | Statement description   | Score     |
| <b>Functionalities of Cloud BI on key data management and security</b>  | The Cloud BI app meets enterprise data management needs   |           |
|   | Most features of the Cloud BI app support current enterprise operations   |           |
|   | The Cloud BI app connects to and supports on-premises data sources or systems                                       |           |
|   | The Cloud BI app can connect to popular cloud data warehouses and databases   |           |
|   | Users interact with the Cloud BI app mainly through the web browsers  |           |
|   | Cloud BI app can run existing on-premises hardware  |           |
|   | Reviews by other customers prove the claims by CSP what the Cloud BI app can deliver                                |           |
|   | The Cloud BI app is built mainly for all different business users   |           |
| <b>Security vulnerabilities, threats and risks in shortlisted Cloud BI app</b>  | Cloud BI can easily be used by non-technical end-users  |           |
|   | The Cloud BI app features that support enterprise data sources, filters, data visualisations are easy to understand |           |
|   | The Cloud BI app has security features to protect data during processing and transit                                |           |
|   | The interface of the Cloud BI is safe, simple and easy to use by non-technical users                                |           |
|   | Cloud BI app interface does not remember access details, particularly passwords                                     |           |
| <b>Security controls in place and their robustness</b>  | Data files from on-premises are compatible with the Cloud BI app and vice versa                                     |           |
|   | The user interface provides strong access control to the Cloud BI app   |           |
|   | Cloud BI app provides for authorisation to authorised users only  |           |
|   | Cloud BI app sessions time-out and automatically terminate all connections  |           |
| <b>Cloud BI's usability by nontechnical users</b>   | Only the administrator can grant access privileges to the Cloud BI app  |           |
|   | The Cloud BI app can be acquired, run, used and audited with much ease  |           |
|   | It is easy to learn how to use the Cloud BI app without formal training   |           |
|   | Online tutorials and YouTube videos on the Cloud BI app are available to assist users                               |           |
|   | Free training is provided for the Cloud BI app  |           |
|   | The learning or training material is relevant to the enterprise needs   |           |
|   | Online experts are available to provide needed support when a client faces challenges                               |           |
| The Cloud BI app is supported by a strong and reliable online community, forums, enthusiast blogs, passionate users or user group   |   |           |
|   | <b>Expected score</b>   | <b>25</b> |
|   | <b>Actual score</b>   |           |
|   | <b>% of Actual score/ Expected score</b>  |           |

(if % < 85%: repeat this process with another CLOUD BI until you find one that closely meets your requirements)

**Figure AP6.2: Checklist 2: Assessing cloud business intelligence usability**

| 3. ASSESSING SERVICE DELIVERY MODELS   |  |           |
|--|--|-----------|
| Name of service delivery service model:.....   |  |           |
| Date of Assessment: .....  |  |           |
| <b>Instructions:</b> These statements represent a checklist of key characteristics to consider when evaluating <b>Service delivery models</b> . Please indicate in the score/answer column whether or not the information provided in the statement meets each criterion for each statement (1 = criterion met; 0 = criterion not met) |  |           |
| Evaluation criteria  | Statement description  | Score     |
| Assess security vulnerabilities, threats and risks for each service delivery model   | There are obvious security vulnerabilities with the service delivery models  |           |
|  | The service delivery model leverage client security control on data and application                                  |           |
|  | The service delivery model is prone to common security threats being reported  |           |
|  | The service delivery model does not affect enterprise current business operations                                    |           |
|  | The vulnerabilities identified are easy to deal with without involving experts                                       |           |
|  | Proper security controls to limit unauthorised access to client's data and information by CSP employees are in place |           |
|  | The service delivery model best suits the enterprise information security needs                                      |           |
| Assess the costs of using each service delivery model  | The service delivery is fairly priced for the CLOUD BI hosting   |           |
|  | The pricing service delivery model fits the budget of the enterprise   |           |
|  | The types of support the CSP will provide, and its cost is clearly stated  |           |
| Assess the knowledge and skills needed for each service delivery model   | Have awareness of different service delivery models issues   |           |
|  | Have skills and knowledge to acquire, provision and audit cloud services   |           |
|  | Aware of existing security threats and risks of the service delivery model   |           |
| Assess financial risks due to security risks in each service delivery model  | There are documented financial risks linked to the service delivery model  |           |
|  | Are the risks covered by CSA and SLAs  |           |
|  | Is the enterprise prepared to accept the financial risks   |           |
| <b>Expected score</b>  |  | <b>16</b> |
| <b>Actual score</b>  |  |           |
| <b>% of Actual score/ Expected score</b>   |  |           |

(Assess the services delivery model (IaaS & SaaS) to suit your expectations % should be 75 to 95%)

**Figure AP6.3: Checklist 3: Assessing service delivery models**

| 4. CLOUD DEPLOYMENT MODELS ASSESSMENT   |   |           |
|---|---|-----------|
| Type of deployment model:.....  |   |           |
| Date of assessment:.....  |   |           |
| <b>Instructions:</b> These statements represent a checklist of key characteristics to consider when evaluating a cloud deployment. Please indicate in the score/answer column whether or not the information provided in the statement meets each criterion for each statement (1 = criterion met; 0 = criterion not met) |   |           |
| Evaluation criteria   | Statement description   | Score     |
| Security vulnerabilities, threats and risks in the cloud  | Cloud allows Cloud BI app to easily integrate with on-premises systems            |           |
|   | Vulnerabilities, threats and risks on on-premises systems are known               |           |
|   | Vulnerabilities in the cloud models are already known or easy to locate           |           |
|   | Threats and risks to the data and application in the cloud are easy to manage     |           |
|   | Any reported security breaches reported for this model                            |           |
| Effectiveness of security controls  | Data segregation among users of different enterprises is provided                 |           |
|   | Security controls to identified threats and risks are in place                    |           |
|   | Security controls are effective against identified threats                        |           |
|   | The cloud deployment model does not disrupt enterprise operations                 |           |
|   | Security controls updated regularly in line with security regulations             |           |
| Availability, reliability and performance of the cloud  | The cloud encrypts all data at rest in databases, file systems and VM layer       |           |
|   | Cloud services are always available most of the time whenever required            |           |
|   | Security in the cloud model is reliable in preventing data breaches               |           |
| Cloud interoperability and application portability  | Performance of the cloud model meets the enterprise expectations                  |           |
|   | Cloud is interoperable with other clouds and on-premises systems                  |           |
|   | Cloud allows applications and data to move to other clouds or on-premises systems |           |
| Data files from the cloud can be accessed easily by on-premises applications without conversion   |   |           |
| <b>Expected score</b>   |   | <b>17</b> |
| <b>Actual score</b>   |   |           |
| <b>% of Actual score/ Expected score</b>  |   |           |

(Set own % of security requirement and assess each cloud deployment model to your expectation. % should be 75 to 95%)

**Figure AP6.4: Checklist 4: Assessing Cloud deployment models**

| <b>5 ASSESSMENT OF CLOUD SERVICE PROVIDERS</b>  |  |              |
|---|--|--------------|
| <b>Name of CSP:</b> .....   |  |              |
| <b>Date of assessment:</b> .....  |  |              |
| <b>Instructions:</b> These statements represent a checklist of key characteristics to consider when evaluating a cloud service provider. Please indicate in the score/answer column whether or not the information provided in the statement meets each criterion for each statement ( <i>1= criterion met; 0 = criterion not met</i> ) |  |              |
| <b>Evaluation criteria</b>  | <b>Statement description</b>   | <b>Score</b> |
| <b>Data governance, accountability and security</b>   | CSP implements and adheres to security policies to protect clients from threats and data losses  |              |
|   | CSP maintains integrity by data encryption to prevent unauthorised access  |              |
|   | CSP preserves data confidentiality with strong authentication to prevent unauthorised access   |              |
|   | CSP uses backup and recovery schemes to maintain the availability  |              |
|   | CSP offers reliable security controls to protect applications and data   |              |
|   | CSP prevents security breaches by denying anonymous users access to services   |              |
| <b>Internal security control through certification and standards for compliance</b>   | CSP has proof of compliance and audit performed regularly  |              |
|   | CSP has proof of data centre protection that enterprises can assess  |              |
|   | CSP keeps a record of end-user log activities as proof of security assurance   |              |
|   | The security standards claimed by CSP are in place and adhered to  |              |
|   | Areas of responsibilities shared between CSP and customer are clearly stated   |              |
|   | CSP can assist the enterprise in meeting compliance standards that apply to industry   |              |
|   | CSP clearly states enterprise responsibilities and support to be given   |              |
| <b>Trust, reliability and history performance</b>   | CSP usually alerts clients of security breaches in the service in time   |              |
|   | CSP provides clients with proof that penetration testing is done regularly   |              |
|   | CSP has robust online communities that depend on the provider's fame   |              |
|   | CSP is readily available to give necessary support to clients who face challenges  |              |
|   | CSP is capable of overcoming most security issues faced by clients who use the services  |              |
|   | The CSP is clear on the type of technical support being given (paid or free)   |              |
| <b>Business continuity</b>  | CSP's technical support is in line with the expectations of the enterprise   |              |
|   | Background checks on possible fraudulent business activities by CSP have been made   |              |
|   | Enterprise data will be safe from security breaches with this CSP  |              |
|   | CSP is capable of attending to system disruptions/outages  |              |
| <b>Cloud service agreement (AUP, SLA and contracts)</b>   | CSP can detect those who engage in malicious or fraudulent activities in the cloud   |              |
|   | CSP has clearly stated or specified intellectual property ownership  |              |
|   | There are clear terms for account termination with the CSP   |              |
|   | CSP reserves the right to share customer data with third parties and condition well stated   |              |
|   | Assess the trust of cloud provider in doing the right thing using a legal agreement that will back up the enterprise if something goes wrong |              |
|   | CSP provides customers with clear information on controls, security and operation of the service on CSA, AUP & SLA                           |              |
|   | Data ownership, shared responsibilities, non-disclosure agreements, dispute handling are laid out clearly and easy to understand             |              |
| SLAs cover essential requirements in terms of availability, response time, capacity and support   |  |              |
| All legal requirements for the security of data hosted by CSP are clearly stated and enforceable by the parties involved  |  |              |
| <b>Expected score</b>   |  | <b>32</b>    |
| <b>Actual score</b>   |  |              |
| <b>% of Actual score/ Expected score</b>  |  |              |

(Set own % between 75 to 95%) CSP security trust, reliability, performance and data governance. Your CSP can be the provider of Cloud BI or host)

**Figure AP6.5: Checklist 5: Assessing security, trust, reliability and performance of CSP**



| <b>5. ASSESSMENT OF FINANCIAL RISKS</b>   |  |  |
|---|--|--|
| <b>Name of Cloud BI:</b> .....: <b>Date of assessment:</b> .....  |  |  |
| <b>Instructions:</b> These statements represent a checklist of key characteristics to consider when evaluating financial risks. Please indicate in the score/answer column whether or not the information provided in the statement meets each criterion for each statement ( <i>1 = criterion met; 0 = criterion not met</i> ) |  |  |
| <b>Evaluation criteria</b>  | <b>Statement description</b>   | <b>Score</b>                             |
| <b>Financial benefits of Cloud BI</b>   | The cost of Cloud BI is substantially lower than acquiring traditional BI            |  |
|   | Costs of training users of Cloud BI apps are lower than traditional BI               |  |
|   | The cost of supporting and maintaining Cloud BI is lower than traditional BI         |  |
| <b>Assess hidden costs</b>  | Initial subscription is clearly stated and fixed                                     |  |
|   | An itemised bill for agreed services can be obtained from CSP                        |  |
|   | Notices of increase in billing are given prior                                       |  |
|   | Clients always alerted of unutilised billable resources                              |  |
|   | Is CSP technical support for free  |  |
| <b>Costs due to downtime</b>  | Expenses for data migration are included   |  |
|   | Only uptime is paid for  |  |
|   | The frequency of downtime does not affect business operations financially            |  |
| <b>Litigation costs</b>   | CSP compensates enterprise for business loss due to outages                          |  |
|   | CSP is fully liable for litigations for data breaches on behalf of clients           |  |
|   | CSP compensates customers for poor services on behalf of clients                     |  |
| <b>Penalty costs</b>  | SLAs have no disclaimers for unauthorised data access and hacking                    |  |
|   | CSP charges fines for any misuse of resources  |  |
| <b>Cost of Cloud BI app</b>   | Penalties resulting from non-compliance and not turning off some services are stated |  |
|   | The Cloud BI app is free of charge or at an affordable cost to the enterprise        |  |
|   | A free trial version is provided for users   |  |
|   | The app easily configured by non-technical users                                     |  |
|   |  | <b>Expected score</b>                    |
|   |  | <b>20</b>                                |
|   |  | <b>Actual score</b>                      |
|   |  | <b>% of Actual score/ Expected score</b> |

(Set own % between 90 to 98% financial safety (2 to 8 % risk acceptance). If the financial risk > 15% repeat the steps 2 to 5 with other Cloud BI app, and providers)

**Figure AP6.6: Checklist 6: Assessing financial risks**

## Appendix L: Tables referenced in Chapter 7

**Table AP7.1: Demographic results of reviewer for relevance validation of the framework**

| <b>Demographic characteristic</b>  | <b>Frequency</b> | <b>Per cent</b> |
|--|------------------|-----------------|
| <b>Highest educational qualification</b>                                 |                  |                 |
| Bachelor of Science in Computing (general)                               | 8                | 42.1            |
| Bachelor of Science in Computing (Honours)                               | 6                | 31.6            |
| MSc in of Science Computing  | 5                | 26.3            |
| Total  | 19               | 100.0           |
| <b>Experience in the IT field</b>  |                  |                 |
| less than 2 years  | 2                | 10.5            |
| 2 to 5 years   | 13               | 68.4            |
| 6 to 10 years  | 3                | 15.8            |
| more than 10 years   | 1                | 5.3             |
| Total  | 19               | 100.0           |
| <b>Knowledge in Cloud business intelligence and other Cloud services</b> |                  |                 |
| Basic  | 4                | 21.1            |
| Good   | 10               | 52.6            |
| Very Good  | 5                | 26.3            |
| Total  | 19               | 100.0           |
| <b>Knowledge in security evaluation in cloud services</b>                |                  |                 |
| Basic  | 6                | 31.6            |
| Good   | 9                | 47.4            |
| Very Good  | 4                | 21.1            |
| Total  | 19               | 100.0           |
| <b>Experience in reviewing IT systems and models</b>                     |                  |                 |
| No   | 1                | 5.3             |
| Yes  | 18               | 94.7            |
| Total  | 19               | 100.0           |

**Table AP7.2: Relevance of evaluation activities for framework component**

(n = 19)

| Activities of each component   | Cluster overall relevance |                 |
|--|---------------------------|-----------------|
|  | Pearson Correlation       | Sig. (2-tailed) |
| <b>Assessment of alignment of data management and security needs to business objectives</b>                      |                           |                 |
| 1.1. Assess alignment of data management plans to business needs   | 0.727**                   | 0.000           |
| 1.2. Classification of data to be migrated, stored, and managed in the cloud on their sensitivity                | 0.750**                   | 0.000           |
| 1.3. Classification of data to be migrated, stored, and managed in the cloud on their security needs             | 0.785**                   | 0.000           |
| <b>Assessing cloud business intelligence security and usability</b>  |                           |                 |
| 2.1. Assess the functionalities of Cloud BI on key data management and security                                  | 0.777**                   | 0.000           |
| 2.2. Assessing security vulnerabilities, threats, and risks in shortlisted cloud business intelligence solutions | 0.608**                   | 0.006           |
| 2.3. <i>Assessing security controls in place and their robustness</i>  | 0.440                     | 0.059           |
| 2.4. Assessing Cloud BI usability by non-technical users   | 0.856**                   | 0.000           |
| 2.5. Assessing the knowledge and skills needed to use each service delivery model                                | 0.815**                   | 0.000           |
| 2.6. Assessing the cost and financial risks of each shortlisted CLOUD BI solution                                | 0.850**                   | 0.000           |
| <b>Assessing cloud business intelligence service delivery models</b>   |                           |                 |
| 3.1. Assess security vulnerabilities, threats, and risks for each service delivery model                         | 0.868**                   | 0.000           |
| 3.2. Assessing costs of using each service delivery model  | 0.877**                   | 0.000           |
| 3.3. Assessing financial risks due to security risks in each service delivery model                              | 0.959**                   | 0.000           |
| <b>Assessing cloud deployment models</b>   |                           |                 |
| 4.1. Assess vulnerabilities, threats, and risks in each deployment model   | 0.485*                    | 0.035           |
| 4.2. Assessing the effectiveness of security controls in place   | 0.616**                   | 0.005           |
| 4.3. Assessing the availability, reliability, and performance of the cloud deployment model                      | 0.869**                   | 0.000           |
| 4.4. Assessing cloud interoperability and application portability  | 0.683**                   | 0.001           |
| 4.5. Assessing costs of each deployment model  | 0.886**                   | 0.000           |
| 4.6. Assessing financial risks of using the deployment model   | 0.856**                   | 0.000           |
| <b>Assessment of cloud service providers</b>   |                           |                 |
| 5.1. Assess vulnerabilities, threats and risks in each deployment model  | 0.753**                   | 0.000           |
| 5.2. Assessing the effectiveness of security controls in place   | 0.557*                    | 0.013           |
| 5.3. Assessing the availability, reliability and performance of the cloud deployment model                       | 0.692**                   | 0.001           |
| 5.4. Assessing cloud interoperability and application portability  | 0.708**                   | 0.001           |
| 5.5. Assessing costs of each deployment model  | 0.831**                   | 0.000           |
| 5.6. Assessing financial risks of using the deployment model:  | 0.849**                   | 0.000           |
| <b>Assessing financial risks due to security risks</b>   |                           |                 |
| 6.1. Assessing hidden costs  | 0.712**                   | 0.001           |
| 6.2. Assessing costs due to downtime   | 0.860**                   | 0.000           |
| 6.3. Assessing litigation costs  | 0.902**                   | 0.000           |
| 6.4. Assessing penalty costs for misuse of services  | 0.833**                   | 0.000           |

\*. Correlation is significant at the 0.05 level (2-tailed). \*\*. Correlation is significant at the 0.00 level (2-tailed)