

The impact of Cloud computing on IT security skills and roles: A case study

ADEKEMI ADEDOKUN

M.Sc Information Security

B.Sc Computer Electronics

A thesis submitted to
Auckland University of Technology
in fulfilment of the requirements for the degree of
Doctor of Philosophy (PhD)

2021

School of Engineering, Computer and Mathematical Sciences

Declaration

I hereby declare that this submission is my work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

.....

Adekemi Adedokun

Acknowledgements

It has been a long, tedious, yet rewarding journey, and I am delighted and grateful for completing this thesis. I am eternally thankful to God for the grace, strength, and blessings to complete this journey.

I want to express my sincere appreciation to my primary supervisor, Dr Brian Cusack, for his dedication, patience, encouragement, guidance, and advice. His tremendous support and commitment made this PhD a success. To my second supervisor, Dr Alan Litchfield, thank you for your support and for always reviewing the research outcomes. Your feedback improved the quality of this research.

I also want to appreciate my friends for their encouragement, prayers, and support during this project. I am greatly indebted to my family for their immeasurable support, prayers, and encouragement in my academic pursuit. To my husband, Paul, and son, James, thank you for your love and understanding; I couldn't have done it without you two.

Abstract

Cloud computing is causing significant changes in the demand and supply of IT skills and the relevancy of current roles. As the IT environment changes with Cloud technology, it is essential to identify and evaluate these changes, and to understand what actions optimise the new business opportunities. Cloud is affecting the way IT roles are constructed and many traditional roles are being changed or discontinued. This is because many of the systems that have been developed and supported by IT staff members are now being replaced by third-party Cloud-based applications and infrastructures, which does not require the support of the same internal IT staff. IT security roles are also changing, and the technical competence requirements are evolving as more is known about the technical implementation of the Cloud. It is an evolving opportunity for businesses, but more is needed to be known about optimal role deployments, security, and the new skill sets required. This thesis aims to explore the changes to IT security skills and roles caused by Cloud computing and the role of Higher Education Institutions in providing the skills.

Currently, there is not enough work in the literature examining the impact of Cloud on skills and roles and how educational institutions can fill the skills gap. Many works are focused on the general perceptions of the barriers of adopting Cloud computing as well as addressing the security issues. Also, there is a wide security skills gap and a lack of Cloud capable security personnel in the industry. This is a research gap that this study intends to fill. This study, therefore, intends to answer the question “what are the impacts of Cloud computing on IT security skills and roles?”

In study, an interpretative case study is used to address the problem of Cloud impacts on IT security roles and skill requirements. Data is collected from three sources – interviews, surveys, and documents, and analysed using thematic analysis techniques in NVIVO. In addition, five sub-questions are developed to help answer the research question. After the data collection is completed, critical reflection is done on the results to inductively generate hypotheses and to identify features in the context for further research.

The findings from the research clusters around the six themes of skills, roles, changes to traditional skills, changes to traditional skills, business benefits, restructuring issues, the role of education, and security concerns. Overall, the research is correct in postulating the significance of Cloud impacts on business decision-making, management actions, and IT service management. Together the findings substantiate the belief that Cloud is having a significant impact on IT service roles and the required business skills for successful management. Finally, in practice, this study contributes to understanding best practices and their continual evolution for education, and business Cloud implementations. Recommendations are made for further research into the evolving industry and academic issues that currently have knowledge gaps.

Publications

- Adedokun, A. & Cusack, B (2021). Cloud challenges for Under-graduate security curriculum, *Australasian Journal of Information Systems* (Submitted).
- Adedokun, A. & Cusack, B (2021). The impact of Cloud disruption on business IT role requirements, *Journal of Computer Information Systems* (Submitted).
- Adedokun, A. & Cusack, B (2021). Skill Deficits Impact Cloud Business Returns, *The Journal of Cloud Computing* (Submitted).
- Adedokun, A. & Cusack, B (2020). Cloud Opportunity and Business Skill Deficits. The proceedings of the 2020 International Business Information Management Association Conference. November 4-5, 2020, Granada Spain. pp. ISBN: 978-0-9998551-5-7
- Adedokun, A. & Cusack, B (2018). Securing wireless vulnerabilities in Wireless Body Sensors. *The Proceedings of the 2018 Cyber Forensic & Security International Conference, August 21-23, 2018, Nuku'alofa, Kingdom of Tonga*, pp.243-254. ISBN 978-1-927184-48-6
- Adedokun, A. & Cusack, B (2018). The impact of personality traits on user's susceptibility to social engineering attacks. *The Proceedings of 2018 SRI Security Congress, December 4-5, Edith Cowan University (ECU)*

Table of Contents

Declaration	ii
Acknowledgements	iii
Abstract	iv
Publications	vi
Table of Contents	vii
List of Tables.....	xii
List of Figures	xiii
List of Abbreviations.....	xiv
Chapter One.....	1
Introduction	1
1.0 INTRODUCTION.....	1
1.1 BACKGROUND AND MOTIVATION FOR THE STUDY.....	2
1.2 AIMS OF THE THESIS.....	6
1.3 SKILLS AND ROLES SEGREGATION FRAMEWORK	6
1.4 THESIS STRUCTURE	8
Chapter Two	9
Literature Review	9
2.0 INTRODUCTION.....	9
2.1 SELECTION PROCESS FOR LITERATURE REVIEW	9
2.2 CLOUD COMPUTING	10
2.2.1 Definition.....	10
2.2.2 Key Characteristics of Cloud	11
2.2.4 Cloud Deployment Models	13
2.3 REVIEW OF CENTRAL AND DECENTRALISE SYSTEM ARCHITECTURES.....	14
2.3.1 Central System Architectures	15
2.3.2 Decentralised Systems.....	16
2.3.3 Cloud Re-centralisation System Architecture	17
2.4 EVOLUTION OF INFORMATION SECURITY SKILLS	18
2.4.1 The Role of Education and Training	20
2.4.2 The impact of the change in the industry	21

2.5	DEFINITION OF TRADITIONAL AND CLOUD IT SERVICE ROLES	22
2.5.1	Definitions of Traditional IT Roles	22
2.5.2	Definition of Cloud Roles	24
2.5.3	Changing Roles in Cloud.	26
2.6	THEORETICAL PERSPECTIVES	27
2.6.1	Disruptive Theory.....	28
2.6.2	Open System Theory	31
2.6.3	Organisation Contingency Theory	32
2.6.4	Resource-Based View (RBV) Theory	35
2.6.5	Contingent Resource-Based View (CRBV) Theory	36
2.6.6	The Conceptual Framework.....	37
2.7	EMERGING CLOUD ISSUES AND PROBLEMS	39
2.7.1	Trust, Security, and Privacy	39
2.7.2	Human Resource and Organisational Capabilities	41
2.7.3	Employment and Downsizing	42
2.7.4	Governance.....	43
2.7.5	Regulations and Compliance.....	44
2.7.6	Risk Management.....	45
2.8	CONCLUSION	45
	Chapter Three	46
	Research Methodology.....	46
3.0	INTRODUCTION.....	46
3.1	A REVIEW OF PREVIOUS STUDIES	47
3.1.1	Four Similar Studies.....	47
3.1.2	PhD on Cloud Outsourcing Impacts	50
3.1.3	SAAS Impacts on IT Department	52
3.1.4	Cloud Impacts on IT Services	53
3.1.5	Cloud Impact on University IT Department	54
3.2	RESEARCH QUESTION	55
3.3	PHILOSOPHICAL ELEMENTS OF RESEARCH.....	59
3.3.1	Ontology.....	60
3.3.2	Epistemology.....	61
3.3.3	Axiology.....	61

3.3.4 Methodology	62
3.4 RESEARCH PARADIGMS.....	62
3.4.1 Positivism	63
3.4.2 Post-positivism	64
3.4.3 Constructivism /Interpretivism.....	64
3.4.4 Critical Realism.....	65
3.5 RATIONALE FOR CHOOSING RESEARCH PARADIGM	66
3.6 RESEARCH APPROACH.....	67
3.6.1 Quantitative Approach	68
3.6.2 Qualitative Approach	69
3.6.3 Mixed Approach.....	69
3.6.4 Rationale for Choosing Qualitative Research Approach.....	70
3.7 RESEARCH METHOD	70
3.7.1 Case Study Method	72
3.8 THE CASE DESCRIPTION	78
3.9 RESEARCH DESIGN	81
3.10 RESEARCH PROCESS.....	83
3.11 THEORETICAL DATA REQUIREMENTS	86
3.11.1 Data Collection.....	86
3.11.2 Data processing	91
3.11.3 Data Analysis	91
3.12 SPECIFIC DATA COLLECTION STEPS	94
3.12.1 Primary Data Collection Steps	94
3.12.2 Secondary Data Collection Steps	96
3.13 SPECIFIC DATA ANALYSIS TECHNIQUES	96
3.13.1 Primary Data Analysis Techniques	97
3.13.2 Secondary Data Analysis Techniques	101
3.14 LIMITATIONS	101
3.14.1 Reliability	101
3.14.2 Validity.....	102
3.15 CONCLUSION	105
Chapter Four.....	106
Results	106

4.0	INTRODUCTION.....	106
4.1	DEMOGRAPHICS	106
4.1.1	Survey Demographics	106
4.1.2	Interview Demographics	109
4.1.3	Documents Demographics	109
4.2	CODE ANALYSIS	110
4.2.1	Phase One – Examining	111
4.2.2	PhaseTwo – Categorizing.....	112
4.2.3	Phase Three – Tabulating.....	114
4.2.4	Phase Four - Findings.....	119
4.3	THEME ONE – IMPORTANT SKILLS	123
4.3.1	Technical Skills	123
4.3.2	Non-technical Skills	127
4.4	THEME TWO – EVOLVING AND NEW ROLES	129
4.5	THEME THREE – CHALLENGES FOR TRADITIONAL SKILLS.....	130
4.6	THEME FOUR – OTHER IMPACT	132
4.6.1	Direct Skills and Roles’ Impact.....	132
4.6.2	Indirect Skills and Roles’ Impact	134
4.8	THEME FIVE– ROLE OF THE HEI	136
4.9	THEME SIX – LEARNING SECURITY SKILLS	139
4.10	DOCUMENT ANALYSIS RESULTS	141
4.11	CONCLUSION	154
	Chapter FIVE	155
	Discussion and Implications.....	155
5.0	INTRODUCTION.....	155
5.1	GENERATING RESEARCH HYPOTHESIS	156
5.2	RESEARCH QUESTIONS	165
5.3	TRIANGULATION OF RESULTS.....	171
5.4	DISCUSSION OF RESULTS	175
5.4.1	Hypothesis Generation	175
5.4.2	The Usefulness of the Hypothesis	177
5.4.3	Research Question Contribution	178
5.4.4	Implications from Triangulation Strategy	180

5.4.5	Result Implications	182
5.4.7	Modified Framework.....	190
5.5	CONCLUSION	193
	Chapter SIX.....	194
	Conclusion.....	194
6.0	INTRODUCTION.....	194
6.1	SUMMARY	194
6.2	LIMITATIONS OF STUDY	197
6.3	RECOMMENDATIONS	197
6.3.1	Cloud Security Education.....	198
6.3.2	Organisations Adopting Cloud.....	198
6.4	FUTURE WORK	200
	REFERENCES	202
	GLOSSARY	222
	APPENDIX A	223
	APPENDIX B.....	224
	APPENDIX C.....	227
	APPENDIX D	232
	APPENDIX E.....	233

List of Tables

TABLE 2.1:	ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING	12
TABLE 2.2:	DESCRIPTION OF TRADITIONAL ROLES	23
TABLE 2.3:	DESCRIPTION OF CLOUD ROLES	24
TABLE 2.4:	TRANSITIONING OF IT SECURITY ROLES AND RESPONSIBILITIES BEFORE AND AFTER	26
TABLE 3.1:	CRITERIA FOR SELECTING A RESEARCH PROBLEM.....	55
TABLE 3.2:	A REVIEW OF RELEVANT QUALITATIVE RESEARCH PARADIGMS	66
TABLE 3.3:	RELEVANT SITUATION FOR DIFFERENT RESEARCH METHODS.....	73
TABLE 3.4:	TYPES OF A CASE STUDY	74
TABLE 3.5:	THE ELEMENTS OF THE CASE STUDY	79
TABLE 3.6:	DATA ANALYSIS PROCESS.....	93
TABLE 3.7:	SUMMARY OF RESEARCH METHODOLOGY	94
TABLE 3.8:	THE COMPONENTS OF NVIVO PROJECT FOR THE STUDY ADAPTED	98
TABLE 3.9:	CRITERIA FOR TRUSTWORTHINESS OF DATA	103
TABLE 4.1:	FIRST SURVEY DEMOGRAPHICS.....	107
TABLE 4.2:	SECOND SURVEY RESPONDENT’S DEMOGRAPHIC	108
TABLE 4.3:	INTERVIEW PARTICIPANT’S DEMOGRAPHICS.....	109
TABLE 4.4:	SAMPLE OF REVIEWED DOCUMENTS	110
TABLE 4.5:	ACHIEVING DATA TRUSTWORTHINESS DURING DATA ANALYSIS	111
TABLE 4.6:	DESCRIPTIVE CHARACTERISTICS	118
TABLE 4.7:	THEME IDENTIFICATION	120
TABLE 4.8:	ANALYSIS OF UNDERGRADUATE PROGRAMS IN SELECTED NEW ZEALAND UNIVERSITIES	142
TABLE 4.9:	ANALYSIS OF PROFESSIONAL SECURITY AND CLOUD CERTIFICATES .	150
TABLE 5.1:	HYPOTHESIS DESCRIPTION	159
TABLE 5.2:	ANSWERS TO RESEARCH QUESTIONS	166
TABLE 5.3:	TRIANGULATION ANALYSIS	172

List of Figures

FIGURE 1.1:	THE RELATIONSHIP BETWEEN TECHNOLOGY, ROLE, AND COMPETENCE	7
FIGURE 2.1:	THE EVOLUTION OF PARADIGM SHIFT AND JOB FUNCTIONS	15
FIGURE 2.2:	CONCEPTUAL FRAMEWORK.....	39
FIGURE 3.1:	STEP-BY-STEP RESEARCH PROCESS.....	85
FIGURE 3.2:	SPECIFIC PRIMARY DATA COLLECTION STEPS.....	95
FIGURE 3.3:	COMPONENTS OF NVIVO PROJECT	97
FIGURE 3.4:	THE STAGES OF USING THE NVIVO PROJECT	98
FIGURE 3.5:	NVIVIO DATA SOURCES	99
FIGURE 3.6:	CREATING NODES IN NVIVO.....	100
FIGURE 3.7:	NODES HIERARCHY ORGANISATIONIN NVIVO.....	100
FIGURE 4.1:	FOLDER STRUCTURE.....	112
FIGURE 4.2:	INITIAL CODING IN NVIVO.....	113
FIGURE 4.3:	CATEGORIZING OF NODES INTO BROADER THEMES	114
FIGURE 4.5:	RESPONDENTS' VIEW ON WHETHER THE TYPE OF CLOUD OR CLOUD SERVICE DETERMINES THE REQUIRED IT SECURITY SKILLS	116
FIGURE 4.6:	RESPONDENTS' VIEW ON WHETHER THE CLOUD IS CAUSING A SIGNIFICANT CHANGE IN IT STAFFING MODEL	116
FIGURE 4.7:	RESPONDENTS' VIEW ON WHETHER SOME SKILLS AND JOBS BECOME IRRELEVANT IN THE CLOUD	117
FIGURE 4.8:	EXPERTS' VIEW ON TRADITIONAL SKILLS EFFICIENCY IN CLOUD COMPUTING	117
FIGURE 4.9:	SUMMARY OF PARTICIPANTS RESPONSE TO THEMES.....	123
FIGURE 4.10:	THE OVERVIEW OF CODES FOR THEME ONE	125
FIGURE 5.1:	SCHEMATIC DIAGRAM FOR HYPOTHESIS GENERATION	158
FIGURE 5.2:	CATEGORIZATION OF THEMES AND RESEARCH QUESTIONS	169
FIGURE 5.3:	DATA COLLECTION TRIANGULATION.....	171
FIGURE 5.4:	REVISED FRAMEWORK	192

List of Abbreviations

AWS	Amazon Web Services
CSP	Cloud service provider
DHS	Department Homeland Security
HEI	Higher Education Institute
IT	Information Technology
IS	Information Systems
InfoSec	Information Security
IAAS	Infrastructure as a Service
KSA	Knowledge, Skills, and Ability
LAN	Local Area Network
NSA	National Security Association
PAAS	Platform as a Service
SAAS	Software as a service
WAN	Wide Area Network

Chapter One

Introduction

1.0 INTRODUCTION

Cloud computing (Cloud) is a model that describes the provisioning of computing services over the internet. Cloud has expanded the scope of information systems, which has led to the development of distributed computing services for various users. This new paradigm shift is beneficial in reducing the cost and time for information management. Cloud mainly depends on resource sharing instead of having applications on dedicated local servers or individual devices.

Jadeja and Modi (Jadeja & Modi, 2012, p. 877) note that the main purpose of the Cloud is to improve the use of distributed resources, combine these resources to achieve higher throughput, and solve large-scale calculation problems. Google, IBM, Amazon, Microsoft, Apple, and VMware have become the top-tier Cloud services suppliers. With the successes of these Cloud service providers, many other companies are also moving to Cloud services. The developments in Cloud services contribute to the uptake in the research and business communities. Several companies, as well as governments, now rely on Cloud services as a solution to reduce costs and improve the quality of their services. It also removes the need for users to plan for provisioning and lets enterprises to start small and only have resources when a service request is received (Puthal, Sahoo, Mishra, & Swain, 2015, p. 116).

Furthermore, as the development of smart devices increases in the market, the use of smart devices for Cloud-based services such as Dropbox, Google Docs, iCloud, and Vine has also gained popularity among individual users. It is gradually becoming an essential part of our daily lives. Moreover, users can access their information from anywhere and at any time without the need to use dedicated machines. Although there are many promising benefits of using Cloud, Cloud technology is disruptive. It has the potential to transform the way business is done in an organisation. Cloud computing is affecting the way IT roles are constructed and many traditional roles are being changed or discontinued. This is because many of the systems that are formally developed and supported by IT staff members are now being replaced by third-party Cloud-based

applications and infrastructures, which does not require the support of internal IT staff. IT security roles are also changing, and the technical competence requirements are evolving as more is known about the technical implementation of Cloud services.

The Cloud is changing the Information Technology (IT) industry, especially with the evolution of roles and knowledge skills. Cloud is redefining existing IT roles and creating new roles, regardless of how organisations view Cloud computing, Cloud computing is causing significant changes in the demand and supply of IT skills and the relevancy of current roles. There is a direct impact on the skills, abilities and roles required by IT security professionals and one of the major issues of adopting Cloud is IT employees' lack of skills and expertise to utilise the opportunity. As the IT environment changes with Cloud technology, it is essential to identify and evaluate these changes, and to understand what actions are required to optimise the new business opportunities. This thesis seeks to examine the impact of Cloud on IT security skills and roles using a qualitative case study research based on data collected from interviews, surveys, and IT course & Professional curriculum.

1.1 BACKGROUND AND MOTIVATION FOR THE STUDY

Cloud is an evolving technology and is becoming more pervasive in the industry, causing a severe change in IT use and organisations. Cloud is changing the IT function from IT service and resource provisioning to overseeing the procurement and delivery of technology from vendors. This revolution is causing a disruption that is felt across every sector, from breaking up traditional business value chains and creating new business models to creating new IT roles and merging or discontinuing existing IT roles, as well as changing the stakeholders' ecosystem. One of the biggest challenges or limitations of adopting Cloud is security and privacy concerns, and many efforts have been made to minimize the threats. Cloud, like every other technology change, introduces new threats that affect the established business models.

The approach to IT security in the Cloud is different from the traditional approach. Cloud is changing the approach for the model for IT security by introducing shared responsibility concepts that are a sharp change from the traditional red and green zones with boundary management for IT security. Security in the Cloud is not the sole

responsibility of an organisation but is shared with the Cloud service provider who is expected to provide underlying infrastructure security. The responsibility is now being shared with the provider or third-party security provider. Security is highly dependent on the Cloud deployment model and services the organisation chooses. Further, one of the most difficult responsibilities of security personnel with Cloud adoption is the challenge of defining the boundaries for responsibility between the user organisation and the Cloud service provider (Adel, Reza, & David, 2013, p. 199). There is a level of complexity involved in implementing security in the Cloud. These are issues such as regulatory compliance and SLA negotiation that make it more difficult to enforce consistent security policies. Therefore, it is essential to understand the issues to successfully implement Cloud security from both parties' perspectives (the Cloud provider and user organisation). Organisational leaders must understand how to handle these changes effectively.

Cloud computing directly impacts the capability of IT security professionals within the organisation and with the Cloud provider. Professionals require unique cloud skills to leverage the potential for performance returns. This also means that user organisations need to build and maintain new skills for working in a Cloud services environment. Organisations' business and regulatory requirements need to be considered before adopting Cloud. For example, Administrators need to upskill to understand how to perform all the necessary security configuration and management tasks. Likewise, Auditor needs new skills to verify the Cloud provider's security compliance. Traditional auditing skills are not efficient and traditional security auditing techniques are not enough to transfer directly to Cloud auditing (Majumdar et al., 2018, p. 12). IT professionals must now manage the organisation's technical issues as well as business and managerial issues. The implications for Cloud on the IT workforce, especially the IT security workforce, are a point of concern for many. A report (Suby & Dickson, 2013), shows that business model changes from the impact of Cloud, would result in a lack of skilled professionals and the need for new job roles. Cloud environments are threatening the relevance of existing IT security employment by changing job roles. McKendrick (2012) reports there is going to be a change in job descriptions with the adoption of Cloud computing and a reconsideration of the

relationships between vendors and user organisations. This is also consistent with Brooks's (2015) findings that anticipated the impact of Cloud would see a move towards increased IT focus on managing vendors, services, and outsourced contracts over the next decade. One of the biggest challenges the IT department is facing is how to prioritize and manage the professional skills transitioning required for the Cloud environment. This transitioning requires a redefinition of existing IT roles and the creation of new roles (Avram, 2014, p. 533).

There is a wide security skills gap and a lack of Cloud capable security personnel in the industry. According to Assante and Tobey (2011, p. 12), graduates generally do not possess the skills needed to meet the growing demands of Cloud cybersecurity positions. The Suby & Dickson (2017) report indicates that there is going to be a 1.8 million IT professional workers shortage by 2022 across the globe because of a lack of skilled personnel. It is due to evolving information security career paths and a lack of understanding of the required Cloud skills (Suby & Dickson, 2017). In their studies, Yeboah-Boateng and Essandoh (2014) note that the shortage of internal knowledge and expertise is rated as the most significant limitation to Cloud adoption, especially amongst Small and Medium Enterprises SMEs (Yeboah-Boateng & Essandoh, 2014, p. 14). Another report notes that the educational system is not adequately preparing the people with the skills needed for the work of the future and the political and economic institutions are poorly equipped to handle these changes (Smith & Anderson, 2014, p. 4). Equipping the educational institution is particularly important as the employee's skills and talents provide a unique source of competitive advantage for an organisation (Huselid, 1995, p. 636). Organisations require unique skills to leverage the Cloud's potential corporate growth (Mitra, O'Regan, & Sarpong, 2018, p. 2). Furthermore, as knowledge and skills are paramount to fulfilling a job function, it becomes paramount to acquire IT professionals with the required skills for the best use of Cloud services.

The present literature has concentrated mainly on identifying the security concerns of users regarding migration to the Cloud. Several studies (Youseff, Butrico, & Da Silva, 2008; Armbrust et al., 2010; Bohm, Leimeister, Riedl, & Krcmar, 2010; Jadeja & Modi, 2012) have analysed the benefits and limitations of adopting Cloud. Many studies exist on exploring the factors affecting the adoption or resistance to Cloud

in organisations (Khan & Malluhi, 2010; Heublein, 2012; Suo, 2013; Hakim, 2018). The previous research indicates that there are security concerns of user organisations in adopting Cloud, and the traditional IT roles are expected to change. Opala (Opala, 2012), in his study, also observes that the manager's perception of security and cost-effectiveness significantly determines the organisation's adoption of the Cloud. However, research shows that one of the least considered factors when migrating to the Cloud is the impact it has on the IT workforce (Brooks, 2015, p. 18). It may be attributed to organisational leaders not making necessary adjustments despite its impact, or a general lack of awareness of the impact, that the Cloud is having on IT staffing. Suby and Dickson (2013, p. 25) also note that there is still a high ambiguity regarding the needed skills for Cloud services. Only a few studies have focused on understanding the skills and roles change. For example, a study by Wood (2017) focuses on understanding IT workers' required skills in managed hosting environments in higher education. He observes that while it is agreed that there is a change in the responsibilities of IT professionals and additional skills are needed, such as increased communication and soft skills, the overall impact of the Cloud is dependent on the leadership and the organisational culture of the institution. Adel et al. (2013) also indicate that IT managers are expected to develop new Cloud management skills as the roles and responsibilities of their current roles are expected to change significantly. It involves a change in the job description and IT department restructuring, including IT personnel moving from individual companies to Cloud service providers.

One of the effective approaches to mitigating these threats that Cloud introduce is to prepare the workforce with new skills and knowledge requirements. There is currently not enough work capturing the skills and roles change for IT security professionals as well as studies examining the role of the educational institutions in bridging the skills gap. This study, therefore, aims to fill this gap by identifying the required security skills for the Cloud and to understand the changes in the roles and responsibilities. It also examines the role of higher educational institutions (HEIs) in adapting to the new technology landscape and filling the skills gap.

1.2 AIMS OF THE THESIS

This thesis aims to explore the changes Cloud is bringing to the way computing services are accessed and provided for business purposes. These changes are impacting the roles required to support IT services and the skill set required. This research is specifically concerned with the changing knowledge and skill set required for IT security roles in the Cloud environment. Hence the research questions are:

- i. What are the IT security skills required by the user organisations for the Cloud environment?
- ii. What are the new and evolving roles for IT security professionals for supporting Cloud computing in user organisations?
- iii. What are the challenges and limitations of the existing IT security skills from the organisation's perspective when confronted by Cloud computing?
- iv. How should security skills be taught and what is the role of HEIs in equipping graduates with Cloud skills?

1.3 SKILLS AND ROLES SEGREGATION FRAMEWORK

This Section explains the relationship between tasks, skills, knowledge, and roles. Roles are a set of business or organisations' functions or duties. The leadership or management of an organisation determines the business needs, then creates a job role to meet the business requirement. A role is a position to the level of a job in an organisation (Heron, 2005, p. 8). A new role has job descriptions, which include the tasks to be performed, and the competencies (KSA) required to get the job done. Tasks are the smallest complete unit of work activity that a job can be divided (Moore, 1999, p. 18).

Generally, competency is made up of the knowledge, skills, and ability (KSA) component. Knowledge generally refers to specific information required to perform a task (Heron, 2005, p. 26). It requires having facts and understanding of a thing, event, or situation and is mainly theoretical. Also, knowledge can be referred to as an abstract intelligence (Winterton, Delamare-Le Deist, & Stringfellow, 2006, p. 25). Skills, however, is the application of knowledge, which is practical. Skills are professional activities or actions performed by an individual to perform organisational duties. Skills

are distinct and based on expertise for a particular task. It measures the level of performance in terms of speed and accuracy at which an individual performs a task (Winterton et al., 2006, p. 26). Competence is a much broader term than skills as it involves the application of a set of skills. It is the combination of skills, knowledge, and activities applied for effective performance in a job. Competence is performance-based and is demonstrated in an individual's actions to meet a task's demands (Hipkins, 2006, p. 2). An updated skill provides individuals with the capabilities to find a job and move around jobs. The impact of technology usually reshapes how work is performed and creates the need for new skills and competence.

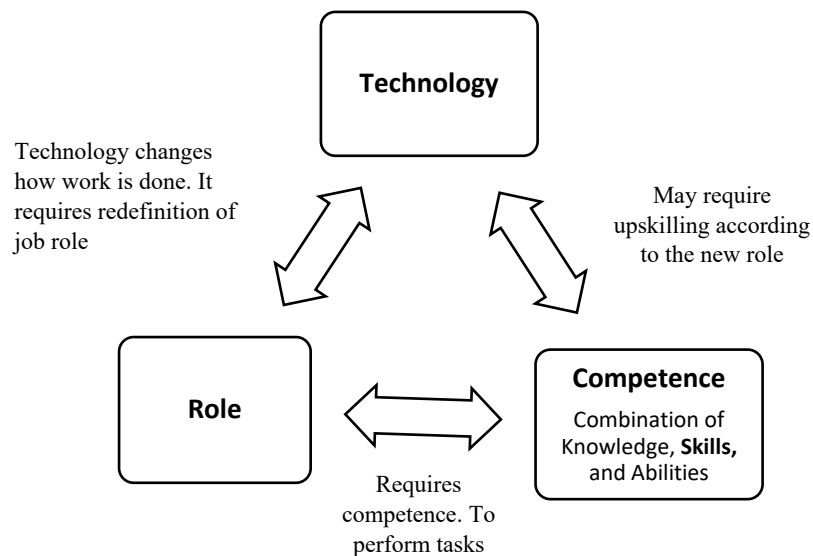


Figure 1.1: The relationship between Technology, Role, and Competence

Figure 1.1 shows the relationship between technology role, competence, and technology. Skills and roles are interwoven, and a change in job roles may require new skills to perform the tasks. This study is focused on the relationship between role, skills, and technology. The aim is to understand how Cloud computing technology has affected the requirement for IT security skills and roles.

1.4 THESIS STRUCTURE

This thesis is divided into six Chapters: The first Chapter of the thesis provides an introductory overview of the study. It outlines the problem background, motivation, and aim of the study. Chapter two is a review of the literature. It focuses on an overview of Cloud computing, decentralised and centralised system architectures, IT service roles, Cloud service roles, and is followed by a discussion on the emerging issues. It also discusses the evolution of information security skills and relevant organisation theory for understanding and interpreting the findings. Chapter three outlines the selected methodology. It looks at the design of this study by identifying studies and choosing the research methodology that is suitable for the study. Chapter three also discusses the problem area identified in the literature. Chapter four presents the findings of the study. Chapter five discusses the findings, limitations, and implications of the study and Chapter six summarizes the research and outlines recommendations for future research. It is followed by a list of references. This is followed by a glossary that defines the key terms used in the study and Appendices for supplementary data used during data collection and processing.

Chapter Two

Literature Review

2.0 INTRODUCTION

Information technology (IT) services are the backbone of business activities as they provide for the effective delivery of products and services. The recent developments in Cloud have led to changes in the way IT services are being accessed and provided for business purposes. Many organisations, as well as governments, now rely on Cloud services to reduce costs and improve the quality of their services.

Chapter two starts with the selection process of the literature review and the definition of Cloud computing. It then examines the existing literature on Cloud, decentralised, and centralised system architectures. It describes the changes in traditional and Cloud roles. It also tracks the evolution of IT security roles and emerging Cloud services issues. Furthermore, it discusses modern organisation theories for explaining organisational changes. The Chapter concludes with a link to Chapter three, which defines the research methodology.

2.1 SELECTION PROCESS FOR LITERATURE REVIEW

This section discusses the literature review selection process for the literature review. The aim of the literature review is to examine the evolution of Cloud technology, security skills, and roles. Also, the review aims to identify the emerging issues and relating to Cloud computing technology. This is done using keywords searching through the AUT digital library and Google scholar search tool.

Keywords searching is a search strategy used for conducting a literature review. The first step of the selection process is to identify the keywords for the study. This was done by identifying the primary words from the research objectives and questions. The keywords and phrases used include impact of cloud, security skills, changing IT roles, changing IT skills, Impact of cloud on IT security, Impact of cloud on IT jobs, Impact of cloud on IT skills, evolution of Information security, evolution of IT technology, and evolution of Cloud technology. The keywords were searched through

the ACM, AIS, Emerald insight, IEEE, Pro-Quest, Sage, ScienceDirect, Scopus, SpringerLink, and Web of Science databases. The keywords were combined in a way that that the database can understand. Also, Boolean operators, parenthesis, wildcards, alternative keywords or synonyms and were used to get a precise and comprehensive result.

The next phase includes choosing relevant publications from the database. The abstract and conclusion of each paper are read to determine if it is relevant. All relevant papers are downloaded from the database and stored for further reading. Each of the relevant paper was then read comprehensively and valuable articles were selected for this study.

2.2 CLOUD COMPUTING

Cloud is a paradigm used to describe the provisioning of computing services over the internet. The concept of Cloud computing can be first traced to McCarthy (1960) when he publicly proposed utility computing, where service providers charge customers for computing resources based on their usage. Cloud computing can be seen as the realization of utility computing. Cloud computing has become a significant technology that is expected to reshape the IT processes and IT market (Furht, 2010, p. 3). The following Section provides an overview of selected definitions of Cloud, key characteristics of Cloud, Cloud services, and deployment models in the literature.

2.2.1 Definition

Several efforts have been made to define Cloud computing. According to Youseff et al. (2008) "Cloud computing can be considered a new computing paradigm that allows users to temporarily utilise computing infrastructure over a network, supplied as a service by the Cloud-provider at possibly one or more levels of abstraction"(Youseff et al., 2008, p. 1). Furthermore, (Furht, 2010, p. 3) defined it as a new form of computing that provides dynamic and salable resources as a service over the internet.

Armburst et al. (2010) defined Cloud computing as "applications delivered as services delivered over the internet as well as the infrastructure and systems that provide the services (Armbrust et al., 2010, p. 50). In an attempt to provide a more holistic definition, Bomh et al. (2010) claim that "Cloud computing is an IT deployment model, based on virtualisation, where resources, in terms of infrastructure, applications

and data are deployed via the internet as a distributed service by one or several service providers. These services are scalable on-demand and can be priced on a pay-per-use basis (Bohm et al., 2010, p. 6). Foster et al. (2008) in their work perceives Cloud computing as: "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualised, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on-demand to external customers over the Internet" (Foster, Zhao, Raicu, & Lu, 2008, p. 1).

Vaquero et al. (2008) provided a more comprehensive definition based on the key features and characteristics of the Cloud. They claimed that "Clouds are a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), also allowing for optimum resource utilisation. This pool of resources is typically exploited by a pay-per-use model in which the Infrastructure Provider offers guarantees by means of customized SLAs" (Vaquero, Roderio-Merino, Caceres, & Lindner, 2008, p. 51).

However, the most widely accepted definition is given by the National Institute of Standards and Technology (NIST) as: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model is composed of five essential characteristics, three service models, and four deployment models" (Mell, Grance, & others, 2011, p. 2).

2.2.2 Key Characteristics of Cloud

Mell and Grance (2011, p. 2) highlight five essential characteristics of Cloud computing:

- on-demand self-service;
- broad network access;
- resource pooling;
- rapid elasticity and scalability;
- measured service;

These characteristics are briefly summarized in Table 2.1.

Table 2.1: Essential Characteristics of Cloud Computing
(Mell et al., 2011)

Cloud Feature	Description
On-demand self-service	Computing capabilities, e.g. server time and network storage, are provided as needed.
Broad network access	Computing capabilities are available over the network and can be accessed through heterogeneous platforms.
Resource pooling	Computing resources are pooled and can be dynamically assigned to serve multiple consumers according to demand.
Rapid elasticity	Computing Capabilities can be elastically provisioned and released and automatically scaled up or down according to demand.
Measured service	Computing Resource usage can be monitored, controlled, and reported
Multitenancy	Services owned by multiple providers are co-located in the same location

2.1.3 Cloud Services

Cloud providers provide Cloud services, and they usually charge users based on their usage. These services, according to NIST, can be broadly categorized into three types: Infrastructure as a service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS).

- *IaaS* provides users with computing resources that are used to support operations, including storage, hardware, servers, and networking components. It is the delivery of hardware as a service to users. The user pays on a usage basis, and the user can control most of the services except the data center. A typical example of IaaS is Amazon's Elastic Compute Cloud (Amazon EC2).
- *PaaS* provides users with Cloud infrastructure where they can build and deliver applications. For this service, the user can control the hosting environment and

the deployed applications. Some examples of Platform as a Service include the Google App Engine, AppJet, Etelos, and Qrimp.

- *SaaS* is sometimes referred to as application as a Service. It provides applications to users on their devices using a multitenancy architecture, and the user is only able to control the Cloud configurations. SaaS allows users to run applications remotely. An example of SaaS is Salesforce.com.

2.2.4 Cloud Deployment Models

NIST further outlines four main deployment models that describe the Cloud environment based on size and access: public Clouds, private Clouds, community Clouds, and hybrid Clouds.

- *A Public Cloud model* refers to a Cloud hosting environment that is accessible to the general public or large industry group. Third parties usually provide them. The public Cloud is owned and managed by the Cloud service provider (CSP), which offers pay-per-use services to customers. This model, however, limits configuration, security, and SLA specification making it less suitable for customers handling sensitive information that is subject to compliance regulations. Rajendra (2013) observes that the implementation of a public Cloud could be of two types: direct approach with CSP bypassing the internal IT organisation or approach through the internal IT department of the organisation (Rajendran, 2013, p. 14).
- *Private Cloud* is sometimes called an internal Cloud, describes Cloud infrastructure that is owned by a single organisation. This model allows individual organisations to have control of their data and infrastructure. There is also a substantial up-front development cost. It is more suitable for organisations that have security and compliance concerns.
- *The Community Cloud model* is designed to serve several organisations that belong to a particular community or group that has shared interests or concerns. The community Cloud may be owned and managed by one or more organisations or by a third party.

- *A Hybrid Cloud model* refers to the combination of two or more models. This model allows organisations to retain control over their resources and still depend on third-party Cloud providers. The following Section describes the development of the emergence of Cloud computing through the different phases of computing evolution.

2.3 REVIEW OF CENTRAL AND DECENTRALISE SYSTEM ARCHITECTURES

Cloud computing has expanded the scope of information technology, which has, in turn, led to the development of distributed computing services to various users. Over the past decades, the evolution of IT follows a progression from a fully centralised approach to a fully decentralised approach and, finally, to a decentralised approach that requires central control. This approach can be divided into three eras: the traditional centralised mainframe business computing; the decentralised movement to PCs, LAN, and WAN; and the internet or Cloud re-centralisation of business computing services.

The centralised systems are expensive for processing large amounts of data and rendering support for several online users simultaneously. This led to decentralised systems where computation is done across multiple systems. The problem with a decentralised system is the difficulty in load balancing and handling system resources to satisfy the user requirements for sharing resources with others. This limitation led to Cloud re-centralisation. Figure 2.1 shows the evolution of Cloud from the era of mainframes. The blue circles describe each era while the orange circles outline the characteristics of each era.

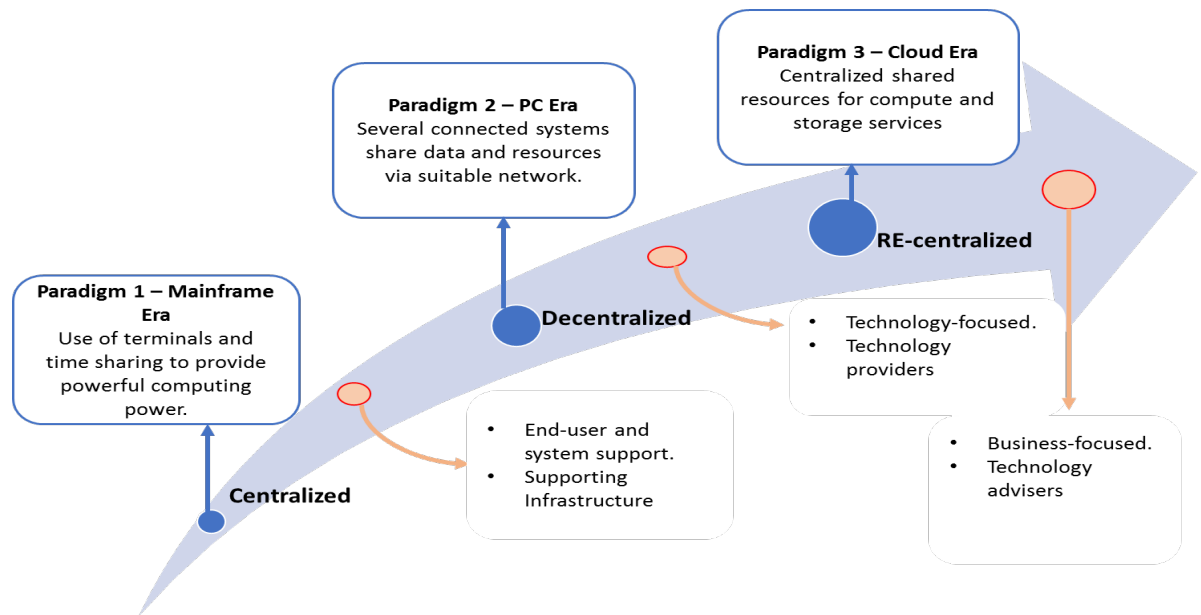


Figure 2.1: The Evolution of Paradigm Shift and Job Functions

2.3.1 Central System Architectures

In centralised computing, a single centralised system performs all the processing of tasks for multiple users. The first computer for business computing is built in the 1940s, and it is the era of mainframes. These computers are large, up to 250 to 1000 square metres, and are designed as business machines to serve as central data repository in an organisation's data processing centre. The mainframes are fully centralised and perform transactions associated with financial statements, billing, accounting systems, etc. (Bento & Bento, 2011, p. 40). They are mostly used by organisations that require processing a large amount of data and the relationship between the user, and the computer system is one-one to one. All the computing processing power, storage, and memory resides on the mainframe and is managed by IT personnel for maintaining security, accounts, backup, recovery, and customer support. Mainframes used batch mode and punch cards for processing tasks. End-users would generally access the central computer through less powerful devices (such as terminals or workstations) and wait for the output in prints or reports. These terminals act as an interface between the user and the mainframe.

Furthermore, centralised systems utilise time-sharing where all computing power may be allocated to a single user when no other user is connected to the system

(Mofaddel & Tavangarian, 1997, p. 3). One of the significant benefits of centralised computing is that it saves customers from having to manage updates. However, centralised computing systems are expensive in terms of processing large amounts of data and rendering support for several online users simultaneously. Then, further advancements and the miniaturization of microprocessor technology facilitated the development of minicomputers. This paved the way for decentralised computing, which can achieve commercial parallel processing. It also saves customers from managing updates for more than one copy of their business data, which increases the possibility of having current data (Ebbers et al., 2016, p. 7).

2.3.2 Decentralised Systems

In decentralised system architecture, the computation is done across multiple systems or subsystems. Several systems are connected to share data and resources via a suitable network. Decentralised systems are a cheap alternative to mainframes. It also provides users with low-cost solutions based on Personal computers (PCs), Local Area Network (LANs), network servers, and multiple microprocessor-based systems (Bohm et al., 2010, pp. 8-9). The idea of PCs is to provide computing to individuals and small businesses with a limited amount of data (Alter, 2000, pp. 380-381). Users are able to store data and run applications on their desktops. Further advancement in miniaturization led to the development of laptops and mobile devices, which brought about extra convenience to users. These smaller machines continue to gain in processing and storage power. The use of networks brought about an organisational approach to the use of PCs allowing people in the same organisation to work together by sharing data and other resources, thus changing the relationship between the user and machine to one-to-many. Several users can access an application running on a machine.

Furthermore, the existence of the internet significantly promotes collaboration and resource sharing between participating organisations, government agencies, HEIs, and private corporations. The rapid advancement of Internet technology in the 1990s paved the way for a new era in information technology. In the mid-1990s, the term grid computing is coined. It refers to a system that coordinates geographically distributed resources that are under the control of various parties, using general-purpose protocols

and interfaces to deliver nontrivial qualities of service (Foster et al., 2008, p. 2). Grid computing aimed to allow organisations to collaborate by solving large scale computing problems by using a network of resource-sharing commodity computers. However, unlike centralised systems, it is quite challenging to manage and control a decentralised organised system as it involves handling system resources in order to satisfy the user requirements for sharing resources with other users as well as balancing the load of the whole system.

2.3.3 Cloud Re-centralisation System Architecture

The advancement of Cloud computing is an evolution of different computing paradigms, which has brought about a change in the way IT services are being accessed. The fundamental concept of Cloud can be traced back to the era of mainframes (Bohm et al., 2010, p. 8). In the Cloud, users no longer compute on their personal PCs or local computers, instead, they use centralised shared resources operated by individual organisations or a third party for computing and storage services. Thus, the Cloud is seen to be a shift to centralised computing as a service.

With the exponential increase in the amount of digital information, there is a higher demand for increased processing power that traditional server and data centre technology cannot address. Cloud can solve Internet-scale computing problems using a large pool of computing and storage resources. Virtualisation is one of the key enabling technologies for the Cloud. It makes it possible to run multiple operating systems and multiple applications on the same server at the same time. Thus, allowing a many-to-many- user to machine relationship. Cloud services are also based on a usage basis, where users can utilise as many resources as they need and only pay for what they have consumed (Foster et al., 2008, p. 1). Cloud allows organisations of all sizes to have access to resources and infrastructures without any capital expenditure.

However, the continually evolving technology also requires a change in IT roles. Cloud computing requires different skills than what most IT employees possess (Bhatnagar, 2015). The need for support employees in an IT organisation is in less demand, as the Cloud is shifting the focus from technical knowledge to service orchestration (Heltzel, 2015). Therefore, IT professionals must ensure their skills

remain relevant to address the new challenges. In the following Section, Cloud and the emerging IT service roles are reviewed.

2.4 EVOLUTION OF INFORMATION SECURITY SKILLS

Information is of great importance to any organisation. Information security has been required from the start of computing, however, the advancement in technology and ubiquitous processing of data has made information security of global interest and importance. It involves protecting information and information systems from unauthorized users. The term information security and cybersecurity are sometimes used interchangeably. However, some authors have argued that cybersecurity includes protecting the human user (Von Solms & Van Niekerk, 2013), while others believe cybersecurity is only concerned with securing cyberspace. The International Telecommunication Union (ITU) refers to cybersecurity as: “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets.” (ITU-T, 2008). For this study, no distinction is made, but the term information security is preferred.

The concept of skills started gaining importance in the 1980s as a result of technological, organisational, and economic factors. Sousa and Rocha (2019) described skills as an individual or organisation resource that allows competitiveness and productivity. Conklin et al. (2014) defined skills as the consistent response that is based on a knowledge component to a particular set of situational criteria. Information security skills refer to the skills needed in ensuring the protection of systems and the information in them. A more comprehensive definition is given by the National Cyber Security Skills Strategy (NCSS), where they defined cybersecurity skills as:

“the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complimentary soft skills that allow organisations to understand the current and potential future cyber risks they face; create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be

followed, upwards and downwards across the organisation; Implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face; Meet the organisation's obligations with regards to cybersecurity, such as legal obligations around data protection; Investigate and respond effectively to current and potential future cyber-attacks, in line with the requirements of the organisation" (NCSS, 2018, p. 20).

Information security in the early years is achieved mainly by controlling physical access to the computer. There is little threat to information, and achieving information security is through computer reliability. It is because computers are expensive, stand-alone with unique software, and controlled by a single person (Cherdantseva & Hilton, 2012). Information security differentiates between what needs to be protected and its environment and has thus relied on perimeter security to protect assets (Pieters, 2011, p. 332). As computers and software production increased in the 1970s, there is also a rise of interest in information security, which brought about a shift from computer reliability to information protection. The need for protecting classified information in the military emerged. With the proliferation of computers in the commercial sector, the need to protect information from unauthorized modification arose. Integrity became the focus of information security. Furthermore, in the 1990s, as the concept and use of the internet became prevalent, the focus of security shifted to internet reliability, which moved the security goal to availability.

Technology is growing at an exponential rate, and it is becoming an integral part of every business. It also means the risk posed is also increasing, and so are the skills needed to cope with these risks. There is a need for a new realization of how information security is viewed in the light of technology advancement, especially with Cloud computing. Information security in the 1950s and 1960s has been treated as a stand-alone corporate asset that only affects the IT department. However, today's cybersecurity involves understanding that security is a business priority and critical to business survival as well as a strategy around technology, process, and education to protect vital resources (CompTIA, 2017). Pieter (2011) argued that the security of an information system is the combination of social and technical mechanisms, and security

solutions should be modelled as such. As technology evolves, the security goals continue to change because new technology poses a different type of security threat. Pieter (2011) further argued that security is socially constructed in a socio-technical constitution of artifacts and humans. Information security is a continuous socio-technical process that needs to be managed (Zaini, Masrek, Johari, Sani, & Anwar, 2018, p. 391). The typical security functions of a security professional in a modern enterprise include a mix of strategic and tactical operations, from deploying and monitoring security controls to incident response, analysis, and forensics (Conklin, Cline, & Roosa, 2014, p. 2). Information security is a fluid environment and professionals need a deep understanding of the technology as well as the security principles.

2.4.1 The Role of Education and Training

Regardless of how organisations view Cloud computing, Cloud is causing a significant change in the required IT security skills and roles in user organisations deploying Cloud technology (Anderson & Gantz, 2012). As the IT environment changes with the adoption of Cloud technology, it is essential to identify and evaluate these changes. However, with this apparent change in technology, it is unfortunate that there is still a wide skills gap in the cybersecurity workforce. It is leading to a current shortage of skilled professionals in the cybersecurity industry. This shortage can be attributed to insufficient exposure to cyber and information security concepts in computing courses at the university, the lack of suitably qualified teachers, and the absence of established career and training pathways into the profession (Furnell, Fischer, & Finch, 2017, p. 6; NCSS, 2018). There is a need to reprioritize the information security skills and cybersecurity education in the light of the current technology to enable professionals to cope in the workforce. The shift in modern security requires a reimagining of workforce development programs and the readjustment of information security skills (Khan & Forshaw, 2017). A recent report by CompTIA (2017) shows that the way organisations view security determines the way skills are assessed and improved.

One of the ways to examine the quality of education available to students is to assess their skills in both academia and industry (Radermacher & Walia, 2013, p. 525). Anderson (2010) observes that there is a shift in the requirement for teacher and student

roles. The teachers are now required to be learning facilitators and knowledge navigators rather than the previously all-knowing authority. Similarly, students are expected to be actively participating in the learning process and collaborate with others to produce knowledge rather than passively receiving information and reproducing knowledge (Anderson, 2010, p. 6).

Academic qualifications and professional certifications are the major sources providing information security and cybersecurity skills. Educational institutions and professional organisations such as the Information Security Consortium (ISC)², Information Systems Audit and Control Association (ISACA), EC-Council, and CompTIA are committed to training professionals to meet the demands of the cybersecurity workforce. The approach to teaching and learning needs to be revised in light of the current dynamic and disruptive technology environment. Leob (2015) in an article, states that “Unfortunately, conventional approaches to cybersecurity training and certification are not keeping pace with the reality of today’s fast-changing and complex technology landscape. Traditional approaches to security training need immediate re-examination, and we must quickly and aggressively boost efforts to educate a new generation of cybersecurity experts.”. There is a wide range of security programs and certifications, which offer different underlying skills and experiences. Educational institutions and industry professionals need to collaborate to have a security competency framework that aligns with the expectation of the employers in the workforce.

2.4.2 The impact of the change in the industry

Organisations face conditions that are frequently changing and require leaders and managers to reevaluate problem and solution activities (Nadler & Tushman, 1980, p. 47). Technology shifts are a major driver of these changes. One of the major impacts of technology disruption in the industry is the global skills gap. Often, the skills gap is used to describe the misfit between graduate skills and the industry’s expectations. The cybersecurity skills gap happens when the security skills workers possess do not align with the required skill to get a task done in an organisation. It asserts that there are insufficient skilled people to meet the cybersecurity needs of an organisation (Cobb, 2016, p. 1).

Employers in the industry define the skills and roles required for employees according to market demands. As organisations adopt Cloud computing technology, there is a change in the skill requirement. Over time, the misalignment of the hiring and training process has been increasing the skills gap (Restuccia & Taska, 2018). Furnell et al. (2017) report that organisations must do their part by distinctively outline what they are looking for in job seekers. The cybersecurity skills gap usually leads to unfilled security job roles due to the shortage of professionals to fill the position. It puts pressure on employees, reduces productivity, and increases the chance of security breaches. Furthermore, organisations should be ready to invest in training and education to help employees upskill accordingly. This addresses the issue of widening the skills gap as well as ensuring the employee's current skills do not become obsolete or redundant.

2.5 DEFINITION OF TRADITIONAL AND CLOUD IT SERVICE ROLES

IT job roles in organisations are rapidly shifting because of the new advances in IT. Cloud computing is a significant digital transformation of how IT services are provisioned. These changes have affected the services, skills, responsibilities, and job functions of IT personnel. Cloud computing technology has simplified IT operations that many roles in IT are becoming redundant and obsolete.

2.5.1 Definitions of Traditional IT Roles

This Section discusses the traditional IT security roles. Generally, the traditional role of IT security professionals in an organisation includes governance and management, auditing and assurance, securing and maintenance of corporate infrastructure, as well as providing recovery for data loss (Ebbles et al., 2016). They operate in a job role such as secure application developers, network and system administrators, information security analyst, operational, recovery. Table 2.2 describes the responsibilities of traditional roles. These roles vary depending on the size and structure of an organisation.

Table 2.2: Description of Traditional Roles

Roles	Responsibilities
Chief Information Officer (CIO)	<ul style="list-style-type: none">• Establishing corporate information policy, standards, and management control over all corporate information resources (Synnott & Gruber, 1981)• Deploying and managing IT in an organisation• oversee the organisation's information resources and ensures information systems is aligned with the organisation's strategy
Chief Information Security Officer (CISO)	<ul style="list-style-type: none">• Integrate security into business processes and strategies as well as balancing business and security objectives (Whitten, 2008, p. 15)• Define security policies and standards, performing risk analysis, performs audits, raise security awareness, and train the operational department on security issues (CIGREF, 2011, p. 129).
Chief Risk Officer (CRO)	<ul style="list-style-type: none">• Oversees the organisation's overall risk profile and access the areas that the organisation is most liable to unexpected loss (Axel et al., 2014, p. 12).• Integrating risk management into the business process and overall strategy, developing and implementing risk assurance strategies to protect against risks associated with the use, storage, and transmission of data and information systems in an organisation.
Security system Administrator (Network, database, storage, server)	<ul style="list-style-type: none">• Maintains the daily operation of security systems• create and modify access rights for user account profiles, install security devices, create security awareness, and maintains security policies and procedures
Service help desk	<ul style="list-style-type: none">• Diagnosing and resolving IT related issues and escalating the issues to next in line technical staff when necessary

System Programmer	<ul style="list-style-type: none"> • Installing, customizing, and maintaining the operating system and its infrastructure in an organisation • Integrating third-party solutions, ensuring system performance tuning is aligned to meet required levels of service (Ebbers et al., 2016, p. 20)
Application Security developer	<ul style="list-style-type: none"> • Designing, building, testing, and delivering of software applications to organisation's users and customers (Ebbers et al., 2016, p. 21)

2.5.2 Definition of Cloud Roles

The senior executive roles of CISO and CIO remain the same in the Cloud with shifting duties and responsibilities. Cloud has introduced new job roles that are not in traditional settings. These jobs generally require new skills and capabilities, and they revolve around supporting the integration process, developing Cloud applications, maintaining and supporting Cloud infrastructure, and collaborating with Cloud vendors to understand the shared security model. Table 2.3 outlines the newly created roles in the Cloud.

Table 2.3: Description of Cloud Roles

Role	Responsibility
Cloud Architect	<ul style="list-style-type: none"> • leading cultural change for Cloud adoption, developing and coordinating Cloud architecture, and developing a Cloud strategy, and coordinating the adoption process (Hilgendorf, 2016, p. 4).
Cloud Engineer	<ul style="list-style-type: none"> • Planning and maintaining the implementation of Cloud infrastructure in an organisation • supporting network administration and integration between on-premises services, Cloud platforms, and Cloud services

	<ul style="list-style-type: none"> • collaborating with stakeholders to improve the network performance, and monitoring Cloud usage
Cloud Analyst	<ul style="list-style-type: none"> • Maintains and reports consumption and works across the technical components and Clouds. • Provide facts for informed decision making and providing reaction to demand changes
Cloud software developer	<ul style="list-style-type: none"> • Designing and developing Cloud distributed software modules that integrate with CSP • Integrating Cloud features into business application development.
Cloud Security Administrator	<ul style="list-style-type: none"> • Strategizing and coordinating internal information security efforts with those of Cloud providers
Security Architect	<ul style="list-style-type: none"> • Evaluate the company as data security in Cloud environments. • Create and design secured layers in the Cloud for ensuring user and data security. • Perform risk assessments as well as mitigating vulnerabilities for Cloud applications (Bhatnagar, 2015).
Network Engineer/Architect	<ul style="list-style-type: none"> • Responsible for implementing, maintaining, enhancing, and providing operational support for network Cloud infrastructure • Creating a flexible networking solution that is capable of scaling to multiple Cloud providers (Bhatnagar, 2015)
Integration manager	<ul style="list-style-type: none"> • Ensures that different Clouds and services are integrated into key delivery processes and ensuring these services meet the business requirement. • Define requirements and plan the integration life cycle.

2.5.3 Changing Roles in Cloud.

The proliferation of disruptive technologies such as Cloud computing is transforming the IT workforce. It is redefining who, how, and where work is done. Technology has evolved from supporting business to empowering and becoming the business (SATI, 2018). IT roles are shifting into a more business-focused position, from adhering to a process that is supported by technology to managing a technology-driven process. Table 2.4 describes some of the transformations in IT roles before and after the Cloud. IT roles are changing from doing the actual technical jobs to thinking of innovative ways to maximize the available technology for maximum business benefits. The concept of security has shifted from the traditional perimeter security of keeping intruders out of the boundary to implementing multiple types of security measures. Security in the Cloud is using a shared responsibility model. The responsibility of the user organisation varies depending on the Cloud service they are consuming. Table 2.4 summarises security responsibility transitions for Cloud.

Table 2.4: Transitioning of IT Security Roles and Responsibilities Before And After

Roles and Responsibility	Before Cloud	After Cloud
Chief Information Security Officer (CISO)	Creating and enforcing policies	Creating and enabling policies
Chief Information Officer (CIO)	Technology-focused	Business-focused
Application development	They are mainly developers and support people.	Involves integrating security into application development and IT Operations concurrently.
Security System Admin / Helpdesk support	Problem solver	Business enabler
Security model	Perimeter security model and solely responsible for end-to-end security	Multi-layered dynamic security view and implements a shared security model
Security Configuration	Manual configuration process	Automated Security configurations

2.6 THEORETICAL PERSPECTIVES

Businesses are exposed to a constant change in the business environment, and understanding the dynamic environment is crucial in achieving the organisation's goals and objectives. Technology's influence is pervasive in organisations and it continues to increase as it provides a competitive advantage (Coover & Thompson, 2013, p. 3). Technology creates new organisational forms and social relations (Orlikowski, 1991, p. 3). Cloud, like every other change in technology, introduces new threats that affect established business models and organisations. The impact of Cloud computing on IT roles is significant. This paradigm shift is introducing new types of market actors and breaking up the traditional value chain of IT service provision. As the business model shifts, there has also been restructuring, redefinition, and redistribution of IT roles and responsibilities. Also, some roles are gradually becoming redundant. Technology has long been impacting jobs. It displaces some and often creates new and higher-skill jobs (Cascio & Montealegre, 2016, p. 355).

Coover and Thompson (2013) indicate that the main issue to consider is not about the technology but rather the focus is on how to manage the impact and implementation of emerging technological innovations. Therefore, this study reviews organisational theories to understand the impact of Cloud on skills, roles, and responsibilities. According to Walsham (1995), the role of theory is very important in any research. Theories are a systematic interrelation of propositions. They are logical explanations of an event, social or natural behaviour, or a phenomenon. These explanations can be idiographic or nomothetic. Idiographic gives explanations to single or specific situations, while nomothetic tends to explain a group of situations or events (Bhattacharjee, 2012, p. 25). A good theory helps the researcher to understand the meaning and intentions of the phenomena studied (Myers, 2019, p. 48). It helps to familiarise the researcher with the subject of study and guides the researchers' focus and interpretations (Kaplan & Maxwell, 2005, p. 37).

A theory is beyond gathering data and facts as it includes explanations, propositions, and boundary conditions (Bhattacharjee, 2012, p. 26). A theory should include four essential elements: propositions, constructs, logic, assumptions/boundaries (Whetten, 1989; Bhattacharjee, 2012). *Constructs* are high-level abstracts

or concepts used to explain a phenomenon. It identifies the “what” of a theory by capturing the factors essential to facilitate understanding a phenomenon of interest. A measurable construct is referred to as a variable. *Proposition* captures the “why” of a theory. It explains the relationships between constructs. *Logic* identifies the “how” of a theory. It captures the rationale for the selection of the factors and the relationship between them (Whetten, 1989, p. 491). Assumptions or boundaries are exemption that governs a theory. It describes the “who, where, and when” of a theory. The concept of organisation theory evolved from the nineteenth and twentieth century in an attempt to explain social and technological changes (Starbuck, 2003, p. 144). To further facilitate understanding of the intended and unintended changes Cloud is having on individuals and organisations, this Section examines related theories to analyse the impact of Cloud computing on IT security skills and job roles. For the purpose of this study, open system theory, contingency theory, resource-based theory, contingent resource-based theory and disruptive theory has been selected to facilitate the understanding of the findings from the study.

2.6.1 Disruptive Theory

The idea that Cloud computing is a new innovation is a controversial topic. Some believe it is a paradigm shift in the way computing services are delivered and consumed while others think it is only a repackaging of existing technology. Regardless of how Cloud computing is viewed, Cloud is causing a change in IT services, and organisations are changing their business models to adapt to the disruptive nature of the Cloud. Aside from other technical issues facing the Cloud, the problem of disruption and disintermediation are causing severe shifts in established business models, and the IT market ecosystem at large. It has resulted in established IT service providers migrating to the Cloud and having to change the main components of their business model. Presently, major vendors including IBM, Microsoft, Oracle, Amazon, to SAP have adopted a Cloud strategy to compete in the market.

The concept of disruptive technology or innovation was introduced by Clayton Christensen (Christiansen, 1997). According to Christiansen, disruptive technologies are innovations that interrupt the prevailing order of things in a particular industry. These innovations occur less frequently, likely to be cheap, simple, and easy to use.

Also, they tend to alter the market dynamics and nature of competition, which may cause established companies to fail. Christiansen further identifies two criteria to identify disruptive technology (Christensen, 2002). First, disruptive technology should enable less skilled or less-wealthy customers to access what only the skilled or intermediary customers could do. Secondly, it should meet the demands of low-level customers who only require limited functionality of existing products in the market. Also, the business model is expected to enable disruptive innovators to realize attractive profits that are unattractive to the current innovators. Cloud seems to be addressing the needs of the current market as it gives an improvement in terms of performance, convenience, price, and flexibility to meet and exceed the market demands (Krikos, 2010, p. 23). Some organisations have sole ownership of computing resources that are unsustainable cost-wise (Krikos, 2010, p. 24).

Moreover, the low-cost utility pricing model of Cloud computing enables it to target those customers that are unable to access such resources and services. Christiansen's disruptive theory is based on the idea that existing companies tend to satisfy and respond to their current customers, thereby failing to commit to new technologies, and eventually end up losing newcomers whose businesses are built around the new trending technology. Cloud has been referred to as disruptive technology as it exhibits all these characteristics (Sultan, 2012, p. 167).

In the past, many organisations that have computing services developed standards to achieve reliability, stability, and security of their information systems (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011, p. 180). They have an established process of delivering and consuming IT resources. However, Cloud is causing a change in IT services, and organisations are changing their business model to adapt to the disruptive nature of the Cloud. This shift in the IT industry is expected to increase the levels of demand for productivity as well as generate significant displacement and creation of wealth from vendor supply of various hardware, software, and application services (Frank, 2012, p. 6). As companies begin to realize the benefits of adopting the Cloud, hardware, and software solutions are being moved to the Cloud, and on-premise servers are being replaced with Cloud data centers.

The companies that provide products to facilitate these data transfers are the greatest beneficiaries (Robb, 2011, 2011), while the existing market that depends on delivering on-premise IT solutions is likely to be severely affected. For example, the data storage market is changing the Original Equipment Makers (OEMs) share, for example, Hewlett-Packard (HP), Dell, EMC, and Hitachi Data Systems. They are likely to suffer loss as their high-end servers begin to compete with companies such as Asian ODM, Foxconn, Quanta, and Wistron. These companies are capable of producing customized datacentre equipment at a lower cost. Other competitors from previously unknown sectors are now in competition in the Cloud market. HP has joined the Cloud industry by including data centers, services, and networking capabilities to their area of specialization to stay relevant in the market. Also, big companies such as Amazon and Google no longer buy branded storage devices but instead, they have opted to have Cloud storage equipment.

Similarly, the traditional software companies market has also been destabilized from its typical up-front payment, on-premise, enterprise-controlled, license-based services business model (Krikos, 2010, p. 29). Generally, the Cloud computing model from the vendor's perspective means a different revenue stream (Hedman & Xiao, 2016, p. 3990). The Cloud model removes the need for: separate maintenance and license fees, solving the complexities involved in software releases, patch management, and human maintenance services between the IT service provider and the enterprise (Krikos, 2010, p. 29). However, the sources of revenue account for two-thirds of major software companies income (Cusumano, 2010, p. 29). Also, one-third of the service revenue is generated from customizing software and patch migration and this is gradually being eliminated (Cusumano, 2010, p. 29). Furthermore, the traditional software delivery model to end customers usually involves several actors but these mediators are being eliminated as Cloud provides software solutions remotely as a service (Boillat & Legner, 2013, p. 49; Hedman & Xiao, 2016, p. 3991),

Furthermore, Cloud computing is changing the stakeholder ecosystem (Clohessy, 2016, p. 36). The traditional IT service provision system consists of two stakeholders, which are the consumer and the provider. However, the Cloud is changing these roles by introducing new enablers to the service provisioning ecosystem (Marston et al.,

2011, p. 182). These changes are bringing about disintermediation. Disintermediation eliminates the need for middle services from business transactions with the hope of improving efficiency for existing products or services. The Cloud computing model is changing the business model for IT service and provisioning.

A vivid example is the change in the way software is being delivered to end-users as compared to the traditional delivery methods. Vendors are gradually being relegated into winners and losers thus bringing levels of disintermediation in the IT market. IT vendors usually work with various partners such as Value-added-Resellers (VAR), who act as consultants, mediators, and retailers for the distribution of their products (Hedman & Xiao, 2016, p. 3991). Furthermore, intermediaries guarantee system performance as they act as system integrators and partners. With Cloud service infusion, the need for this kind of partnership is being eliminated as the Cloud model provides opportunities for IT vendors to sell directly to their customers. The problem with removing middlemen is that it poses a lot of challenges such as job loss, lack of transparency in the market, and the possibility of price hikes by the producers.

The disruptive Cloud model is displacing some businesses while others are benefitting from this business model. Although not all big organisations are yet to embrace the Cloud, the Cloud is the preferred solution to many retail challenges (IBM, 2010, p. 3). It is not clear the role of traditional IT partners such as the VARs in the Cloud, as the Cloud is currently a threat to the present software licensing companies (Krikos, 2010, p. 22). However, as it appears, the Cloud is here to stay, and the best way to harness the power of disruptive business models is to manage the technology as an integrated stack and enable business models by using this integrated technology stack (Frank, 2012, p. 8). Therefore, it is crucial to thoroughly analyse the Cloud's ability to meet business needs before its adoption as the success or failure of a business is dependent on it.

2.6.2 Open System Theory

System theory is an organisational theory that views organisations as a system. It provides a framework to understand change and complexity in nature and the human-constructed world (Chen & Stroup, 1993, p. 447). Organisations are viewed as open or closed, depending on how they interact with their environment. A secure system is

focused on the internal structures and behaviours, it is not affected, and has no interactions with the external environment. Open systems are dependent on the external environment and are focused on maintaining external interactions to survive (Cummings, 2015, p. 893).

The basis of open system theory is that an organisation has similar characteristics with other living things (Hanna, 1997, p. 14). The concept of open system organisation is conceived by Katz and Khan (1966). They viewed the organisation as subsystems of one or larger systems from which they receive energetic inputs, and for which they produce energetic or product outputs (Abbott, 1967, p. 101). The theory emerged as a means of defining an organisation's effectiveness by its dynamic interaction with its environment and internal forces (Sanders, 2002). It posits that the success of an organisation is dependent on the cooperation of interactions and interdependence of different subsystems and its environment. Open system theory emphasises the concept of boundaries and goals. A goal is a purpose for which a system or organisation exists. At the same time, the boundary is an essential element that differentiates a system and its elements from its environment and other systems.

There are basic elements of open system theory: *inputs, transformation process, output, feedback, and environment* (Hanna, 1997). Inputs are the resources and energy an organisation gets from the environment. The process is the steps involved in transforming the raw materials and energy into products that are exported to the environment and other internal use. Outputs are the materials, products, and energy generated from the system to be exported into the environment. Environment refers to anything outside the boundary of an organisation. Open system theory is beneficial to organisation description in the current dynamic and unstable Cloud environment. The environmental factors that influence the system can be classified as specific or general. Nearly all modern organisation utilises an open system. This ranges from institutional theory, resource dependency theory, contingency theory etc (Bastedo, 2004).

2.6.3 Organisation Contingency Theory

Contingency theory is an organisational theory that defines an approach that the structure of an organisation is dependent on the organisation's technology and environment. It is one of the most widely used theories in studying an organisation. It

relates to modern organisations as it explains the behaviour of both an organisation and its employees (Al-Abbadi, 2015, p. 129). The theory arose as an alternative to the ideal single organisational structure. Organisations are viewed as open systems that interact with the context in which they function and in which structures are expected to vary depending on their context (Child, 1975). Paul Lawrence and Jay Lorsch are credited with the contingency theory. They postulate two assumptions. First, there is no single efficient organisation structure, rather organisation structure for each organisation is contingent on internal and external factors such as technology, market, and task predictability. The second assumption is that any way of organising is equally not effective (Galbraith, 1973).

Contingency theory emphasizes that the growth and effectiveness of an organisation are dependent on maintaining adapting activities with the subsystem and environment. It allows organisations to respond to situational variables to achieve their goals. It enables the study of organisational behaviour, as it explores the impact of both external and internal contingent variables such as technology, culture, and the environment on functions and design of the organisational structure (Abba, 2018). For contingency to be effective, it should be dependent on the context in which the organisation operates (Kalchschmidt, 2012, p. 784). A change in the environment is causing a misfit with the organisation structure, which results in low performance. Environmental factors could include suppliers, customers, competitors, government regulatory agencies, and public pressure that are outside the organisation (Ma & Ratnasingam, 2008).

Contingency theory has been applied to various fields of study, and information security is one of such field (von Solms, Van Der Haar, von Solms, & Caelli, 1994; Petroni, 1999; Hong, Chi, Chao, & Tang, 2003; Ma & Ratnasingam, 2008; Twala & Kekwaletswe, 2019). Hong (2003) proposed an integrated system theory based on a contingency theory to integrate security policy, risk management, internal control, and information auditing as a sequential process to meet the organisation's objectives in a fast-changing environment (Hong et al., 2003, p. 247). They believe that contingency processes usually originate from security management activities before proceeding consequentially. Similarly, Ma and Ratnasingam (2008) proposed a conceptual model

that lists the factors for achieving Information Security Management (ISM) objectives. These are security readiness, organisation context, and environmental context. Their model provided a guideline for management that ISM is an evolving process, and an organisation should be ready to effect necessary changes to improve the ISM mechanism (Ma & Ratnasingam, 2008).

With the advancement in technology such as Cloud services, where the role of people and the environment is highly dynamic, contingency theory is relevant to organisations adopting Cloud computing where the security skills and roles also need to adapt to this new environment. Several studies have applied contingency theory to Cloud adoption in organisations (Weber & Otto, 2007; Winkler, Goebel, Benlian, Bidault, & Günther, 2011; Bounfour, Fernandez, & Waller, 2015; Barrett, 2017; Victor, 2020). A more recent study focused on the conceptual framework for Cloud adoption. The framework is made up of the external environment, stakeholders, contingencies, organisational, and technology (Twala & Kekwaletswe, 2019). Their framework emphasized that stakeholders influence Cloud use and adoption. An IT strategy has to be aligned with the business strategy for the smooth adoption and use of Cloud in an organisation (Twala & Kekwaletswe, 2019).

Information security contingency theory involves considering both internal and external environments to determine the best security strategy for an organisation (Tassabehji, 2005). Also, it should include prevention, detection, and the reaction to threats and vulnerabilities, and their impacts both inside and outside of an organisation (Hong et al., 2003, p. 245). Also, Pieter (2011) explained that the internal and external environment determines the threat and how to protect information systems, and people play a major role in the threat and protection process (Pieters, 2011, p. 327). Information security has evolved from a single path solution where the perimeter separates the organisation from its environment. While the concept of perimeter security may still be relevant today, it is no longer homogeneous but context-dependent. The derived model has all possible interactions between information items (Pieters, 2011, p. 332). The attacker is also considered as part of the perimeter and the actual security level is based upon the perceived security requirement.

2.6.4 Resource-Based View (RBV) Theory

The resource-based view emerged from accounting for evaluating the differential performance of organisations within the same environment (Barney, 1991; Mitra et al., 2018, p. 3). It has become one of the most cited theories in management (Kraaijenbrink, Spender, & Groen, 2010, p. 350). The main concept of RBV are resources, capabilities, and strategic assets (Barney, 1991). RBV argues that an organisation can gain a competitive advantage by managing its strategic resources. Barney (1991) defined resources as physical capital resources (the equipment, raw materials, and location), human capital resources (skills, relationships, and people), and organisational capital resources (structure, planning, controlling, and coordinating systems). These are controlled by an organisation to enable the organisation to develop and implement strategies that improve its efficiency and effectiveness (Barney, 1991, p. 101). The resources must be valuable, rare, perfectly aligned, and non-substitutable (VRIN) attributes to achieve a sustained competitive advantage (Barney, 1991, pp. 105-106). RVB focuses on the internal sources of competitive advantage in an organisation and aims to explain the differential performance of organisations in the same Industry.

RVB theory is based on two basic assumptions: first, the organisation's resources are heterogeneous. The second is that resources are immobile. While the first assumption helps explain why organisations may have different implementations of capabilities, the second assumption is unrealistic in a modern business environment. It is explicitly reductionist and against emergent theories that view organisations as organisms with complex feedback-controlled mechanisms focused on boundary maintenance (Kraaijenbrink et al., 2010, p. 351). RBV has been widely adopted in the IT Industry with a focus on using IT resources and capabilities to achieve competitive advantage (Son, Lee, Lee, & Chang, 2014, p. 654). However, many studies have argued that IT resources are widely available and can be easily sourced (Teece, Pisano, & Shuen, 1997; Kraaijenbrink et al., 2010; Son et al., 2014; Mitra et al., 2018). Similarly, with the rapid development of technologies, such as Cloud, there is a market for organisations with up-to-date skills (Mitra et al., 2018, p. 3). Kraaijenbrink (2010) argued that RBV is not effective in a dynamic environment because the resource

attributes are not sufficient for explaining and achieving a sustainable competitive advantage. (Kraaijenbrink et al., 2010, p. 351).

In the case of Cloud, uncertainties and scarce resources are external factors and are beyond the control of decision-makers (Nemati, Bhatti, Maqsal, Mansoor, & Naveed, 2010, p. 113). It has been argued that resources can be acquired from the market or created by the organisation, but competencies and capability need to be developed within the organisation through the combination and integration of resources which requires some level of complexity (Brush & Artz, 1999, p. 225; Jeble et al., 2018, p. 516). Cloud competencies require constant adaptation and change which are related to the maturity levels of Cloud implementation in an organisation. This is dependent on the skills and how the staff implements Cloud. Hence, varying distinctive skills are identified in the various organisation implementing Cloud (Mitra et al., 2018, p. 5 & 7). Although studies have shown that IT capabilities are driven by complex factors and may not be necessarily rare, IT capabilities can influence the success of Cloud deployment and help a firm to achieve a competitive advantage. But the factors determining the IT capabilities are complex (Son et al., 2014; Garrison, Wakefield, & Kim, 2015; Mitra et al., 2018).

2.6.5 Contingent Resource-Based View (CRBV) Theory

Contingent resource-based view is a combination of RBV and contingency theory. The term contingent resource-based theory is coined by Brush and Artz (Brush & Artz, 1999). The CRVB is developed to address the limitations of the VRIN attributes of resources for achieving competitive advantage. The VRIN attributes are impracticable and context insensitive as it omits the contingency factors used in identifying the value of resources. Brush and Arts (1999) argued that the resources needed to achieve competitive advantage vary across different goods and services which includes experience, credence, and service qualities. (Brush & Artz, 1999, pp. 223-224). Also, contingency theory clearly explains that different environmental factors require a varying level of management decisions and strategy for optimum performance (Hofer & Schendel, 1978). It is important to note that while the environmental factors can affect the strategy and performance of an organisation, it does not automatically determine it (Aragón-Correa & Sharma, 2003, p. 73).

A CRBV argument is that an organisation's internal resources are not sufficient in achieving competitive advantage, because it is dependent on the external environment as well as strategy (Ling-Yee, 2007, p. 361). CRBV is focused on the alignment of internal resources with environmental factors to achieve optimum performance. CRBV has been widely used in studying the impact of IT on an organisation's performance to address the limitation of RBV theory (Aragón-Correa & Sharma, 2003; Cao, Wiengarten, & Humphreys, 2011; Roy & Khokhle, 2011; Jeble et al., 2018). Overall, the tenets of RBV theory is on utilising internal resources and capabilities that impact an organisation performance for achieving competitive advantage. Contingency theory stresses having a fit between the internal factors and external environment to achieve optimum organisation performance. From a resource-based view and contingency theory perspective, this study aims to develop a framework for the impact of Cloud computing on IT security skills and roles in an organisation and how it effects the performance of an organisation.

2.6.6 The Conceptual Framework

The conceptual framework is useful in data collection and analysis for explaining the main components to be studied. It highlights the key factors, constructs, or variables as well as the relationships between them. It can be theory-driven, elaborative, descriptive, or casual (Miles & Huberman, 1994, p. 18). While a conceptual or theoretical framework does not necessarily generate good qualitative research, a conceptual framework can be used as a guide in designing the study and for developing a framework (Green, 2014, p. 36). The conceptual framework for this study is informed by the theories discussed in Section 2.6. The framework explains how the characteristics of a Cloud business environment may affect the people, transform roles, skills, and capabilities required for an organisation. The underlying application of theory to this study is to help understand the appropriate security skills and roles, as well as essential knowledge that is the best fit for the Cloud environment. The conceptual framework is, however, only a working framework subject to change with the possibility of finding contrary results when the data is inductively analysed. With the advancement in technology, and where the environment is highly dynamic, the strategy, security skills, and roles also need to adapt to this new environment to achieve

a competitive advantage. Figure 2.2 presents the conceptual framework for this study. The framework is based on the tenets of the disruptive theory, contingency theory and resource-based theory. These theories were selected because they capture the organisational changes and the dynamics that result from cloud adoption within and outside the organisation. Skills and roles change are parts of the impacts of adopting Cloud in an organisation.

In the model, an organisation is viewed as an open system that constantly interacts with its environment. The framework considers Cloud computing as a disruptive innovation, which is changing the landscape of businesses. Cloud is introducing new delivery models and restructuring the IT industry. These changes require organisations to strategise and come up with a creative process to maximise the benefits of Cloud. Based on Contingency theory, an organisation should be contingent on internal and external factors such as technology, market, and task predictability. For organisations to maximize the benefits of the Cloud successfully, the leadership must be willing to re-align the organisation's strategy and to adapt to the contingencies produced by the changing environment. The environment is characterised by Cloud services, Cloud deployment models, competition from CSPs, and regulations from governing bodies such as the government or industry. The organisation transformation process includes the fit between the strategy and organisation processes and understanding the roles and responsibilities in achieving the organisational goals. It includes the definition of who is responsible for security, what are the changing roles, which job responsibilities need to be reviewed or redefined, and what are the skills requirements, and so on. Also, the staffing model (the hiring and restructuring), knowledge, and skillsets to evaluate the competence of current staff. Considering the aim of this study is to examine the direct impact of Cloud on an organisation in terms of skills and roles change, the framework also builds on the tenets of CRBV theory that emphasises on aligning the internal resources such as IT capabilities can influence with the changing environment for a better competitive advantage.

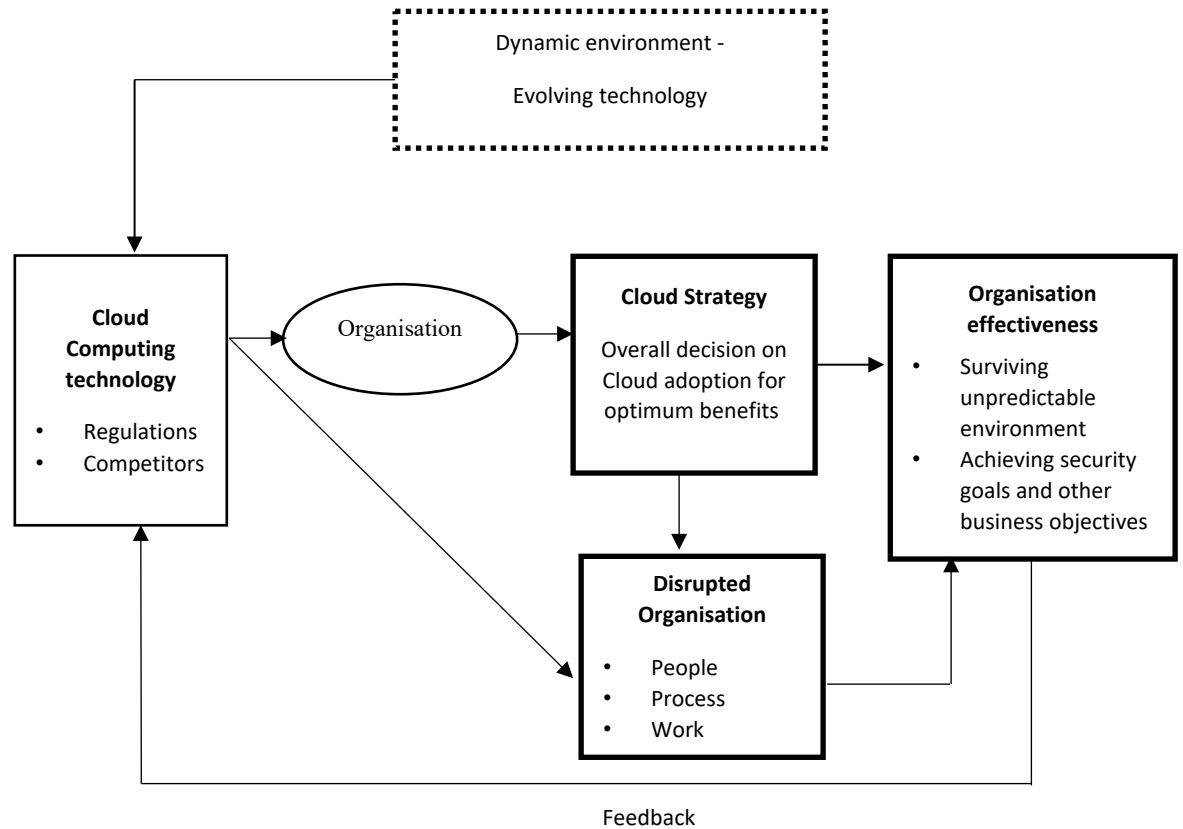


Figure 2.2: Conceptual Framework

2.7 EMERGING CLOUD ISSUES AND PROBLEMS

Though there are many benefits and compelling features of Cloud computing for users and organisations at large, such as accessibility, improved performance, reduced cost through resource utilisation, etc., it also comes with its unique challenges. The following Section describes the challenges of adopting Cloud in an organisation.

2.7.1 Trust, Security, and Privacy

Although there are several promising benefits of using Cloud, weaknesses such as information security and privacy issues, loss of user control, and trust management are still major issues hindering the growth of Cloud computing. There is an increasing concern among Cloud users that the Cloud is becoming a target for hackers. Cloud users have raised concerns about the security of their data stored in the Cloud.

Unfortunately, relying solely on CSPs and legal agreements to fulfil their claims of ensuring a secure Cloud is not sufficient to increase the user's confidence. Past events of personal data breaches have proven to be material risks, even for reputable Cloud providers (Vascellaro, 2009; Singel, 2011; Berghel, 2012; Gordon, Fairhall, & Landman, 2017). These incident reports have increased user's distrust towards Cloud computing. With security in the Cloud, the security mechanisms are unverified, and users need to rely on SLA (service level agreement) trust that Cloud providers provide the needed security. The Cloud-specific standards, such as FedRAMP, HITRUST, and ISO 27018, have only been recently developed. They might take some time before they are relied upon to provide effective Cloud security assessments and reliability. Some Cloud providers have already started certifying against these standards (Peake, 2018). Chiregi et al. (2017) note service quality, security, privacy, trust, integrity, and reputation as some of the most critical issues in Cloud computing (Chiregi & Navimipour, 2017, pp. 3-4).

Similarly, the authors in (Srinivasamurthy, Liu, Vasilakos, & Xiong, 2013) reveals that achieving security in Cloud computing involves five goals: availability, confidentiality, data integrity, control, and audit. CSPs store user's private information such as health records, credit card information, access credentials, and other sensitive data in back-end databases and file systems, which are usually beyond the user's control. This usually raises trust and security concerns for users as there is no transparency on what happens to their data or who can access their data due to its third-party nature and high risk of unauthorised access.

Pechardscheck (2012, p. 3), reported that trust is the primary determinant to the adoption and growth of Cloud computing as there is no business without trust. The work in (Xie, Liu, Cheng, Hu, & Ni, 2016) describes trust evaluation as a mechanism to guarantee service quality. Also, Chen et al. (2010, p. 4) show that Cloud computing introduces new security issues such as the complexities of multi-party trust considerations and the need for mutual auditability. Furthermore, Khan and Malluhi (2010, p. 20) indicate that it is essential for Cloud providers to be more transparent about their services and offer more consumer control of data to earn user's trust. In Zavou (2015, p. 2), the author defined trust to be the level of confidence Cloud users

have in using Cloud services based on the level of transparency, degree of control, and the provider's reputation. They claim that providing efficient auditing capabilities across the whole Cloud infrastructure would increase the user's trust regarding confidentiality breaches, information leaks, and Cloud transparency. Utilising Cloud services to store confidential data should not remove the requirement for its protection with the same diligence as the traditional system. In fact, more stringent measures should be in place.

Cloud users are likely to trust service providers with more transparency in their internal operations. Also, users tend to require more assurance apart from the signed legal agreement that their data is being used as expected and to be informed when there is a breach of security. However, due to the complex nature of Cloud computing and the non-translucency nature, it gives room for an increased attack surface and makes data security in the Cloud a difficult task.

2.7.2 Human Resource and Organisational Capabilities

Technology has long been impacting human resource management. Cloud computing, like every other technology, has affected the human resource processes and functions such as recruitment, training, performance management, benefits, etc. (Johnson, Thatcher, & Bursleson, 2016, p. 228). It has been argued that the advances in Cloud computing are as much dependent on the organisation structure processes as it is with technology (Fellows, 2008). Cloud tends to destroy competencies, organisation structure, and processes, increase task uncertainty and may change the business identity (Ciborra, 2009, p. 134). The adoption of the Cloud involves an ample redefinition of existing IT roles and the creation of new positions. As with other technologies, there is usually a re-allocation of workers between different skill groups within and across organisations (Bauer & Bender, 2004, p. 2). Identification of which skills and roles are needed in the new environment for individuals and organisational responsibilities are open issues arising. IT roles are changing from doing the actual technical jobs to thinking of innovative ways to maximize the available technology for maximum business benefits. Avram (2014) outlines that there are two aspects to a technology shift; the first is concerned with acquiring new skill sets to deploy the technology to solve a

business problem, and the second is how the technology changes the IT role (Avram, 2014, p. 533). Most organisations have focused on the other benefits of the Cloud, with little emphasis placed on the impact Cloud has on the human resources or organisational capabilities (Avadikyan, Lhuillery, & Negassi, 2016, p. 278). Cloud improves HR efficiency and reduces cost, but it may also reduce the need for internal IT staff (Johnson et al., 2016, p. 232). It affects the nature of jobs, job relationships, and supervision (Stone, Deadrick, Lukaszewski, & Johnson, 2015, p. 217). Also, with the adoption of the Cloud, Cloud applications come with their support, separate from corporate IT. Depending on the type of Cloud deployment used, there are changes in the internal processes, responsibilities, and skillsets of the employees (Cheon, Grover, & Teng, 1995). For example, system support service within the organisation may no longer be required in a Cloud environment as they are no longer in control of the infrastructure. Furthermore, Golson (1977) reveals that organisations need new types of managerial, diplomatic, and social skills and a new decision-making process that is not accommodated in the existing organisational structure. He argued that these changes need to be implemented not because they are helpful but because it is necessary for an organisation to continue to exist (Golson, 1977, pp. 293-294). Also, Ranjendra (2013) claims that organisations need two types of skills: first, is the competence in contract management, and the other is understanding governance structures and business processes (Rajendran, 2013, p. 18).

One of the major issues of adopting Cloud is the lack of required skills and expertise by IT employees. An organisation's efficiency is based on the extent of skills, motivation, and the readiness to exploit such opportunities (Ciborra, 2009, p. 134). Yeboah-Boateng and Essandoh (2014), in their studies, show that the shortage of internal knowledge and expertise is rated as the biggest limitation to Cloud adoption, especially amongst Small and Medium Enterprises SMEs (Yeboah-Boateng & Essandoh, 2014, p. 14).

2.7.3 Employment and Downsizing

With the evolving roles and skillsets needed in the Cloud, there is a likelihood of downsizing current employees and hiring new workers with the required skills. Some existing IT job roles are becoming oblivious as the Cloud is now handling them. Some

of these roles are being made redundant, while others are being commoditized, outsourced, and paid for as per use. Also, several individual roles are being merged into a new job role in the Cloud. It affects the employment rate in the IT department. For example, Rajendra (2013) observes that when organisations deal directly with CSPs to meet their IT needs, it may result in some existing roles becoming obsolete as organisations and their IT department has little role to play when there is a change in the control rights, decision rules, governance and cultural structure (Rajendran, 2013, p. 15).

Without a doubt, the total number of full-time employees in corporate IT are decreasing (Seay, Washington, & Watson, 2016, p. 661). Similarly, McAfee and Brynjolfsson (2014), in their opinion, foresees a jobless future. The authors note that new technological change would destroy jobs on a massive scale. However, as some roles are being scrapped, new roles are also being created. This technological change creates phases of job destruction. Eventually, a lot of new and better jobs are created (Mokyr, Vickers, & Ziebarth, 2015, p. 47). Similarly, Cascio & Montealegre (2016) reveals that there would be concurrent unemployment and the creation of new job roles. As roles shift and unemployment rise because of the structural shift in the economy, workers would have to adjust their skills and entrepreneurs create jobs using the new technology (Cascio & Montealegre, 2016, p. 355). Furthermore, advances in technology may displace some types of jobs, but historically they have been known to create jobs. Also, people have to adapt to these changes by creating entirely new types of work and the use of their human capabilities (Smith & Anderson, 2014, p. 1).

2.7.4 Governance

Cloud is resulting in many changes throughout an organisation. There is no doubt the IT department are affected the most with these changes as they are responsible for IT service provisioning in an organisation. It has been the case with other changes in technology. The Cloud model involves interacting with multiple parties, which in turn makes controlling and maintaining the IT risks a complex task (Avram, 2014, p. 533). The redefinition of processes, organisation culture, and structure requires new forms of governance and management.

Also, IT leaders are still accountable for delivering quality of service even when the Cloud reduces control over those services (Marquis, 2018). The CIOs are responsible for controlling end-to-end IT decision-making in an organisation. However, with advances in the Cloud, where most of the infrastructures are outsourced to one or multiple service providers, the CIO role now involves managing and controlling a more complex IT environment (Bob, Geoff, & David, 2011, p. 2). A lack of a clearly defined governance mechanism could lead to ambiguity in decision-making, leading to low performance (Rajendran, 2013, p. 18). Furthermore, Cloud computing requires maturity in management; therefore, the migration approach to the Cloud requires careful identification of how the Cloud could influence the IT governance policies (Bounagui, Hafiddi, & Mezrioui, 2014, p. 3)

2.7.5 Regulations and Compliance

One of the most common compliance issues is data location. Currently, Cloud stores a user's data in a shared environment collocated with data from other customers (Jansen, 2011, p. 5). Some organisations require that users or sensitive corporate data be stored in the same geographical location. This is especially important to an organisation that is handling regulated data (Jaeger, Lin, Grimes, & Simmons, 2009; Joint, Baker, & Eccles, 2009; Mowbray, 2009). Regulations and compliance for where data is located geographically in the Cloud may not be known.

It becomes challenging to ensure that the legal regulations and security compliance are met when the data have crossed national borders where different laws and regulations apply (Jansen, 2011, p. 6). Similarly, organisations are highly concerned about disaster recovery plans. Since CSPs store the user's data across multiple servers in different locations, it is unclear what happens in case of a server failure and the possibility for recovering data. Furthermore, project management is being affected as people are gradually bypassing the authority of the IT department to use the Cloud. Project managers are progressively replacing the services provided by the IT department with Cloud services (Khajeh-Hosseini, Greenwood, Smith, & Sommerville, 2012, pp. 449-450).

2.7.6 Risk Management

Risk management is another factor that needs to be critically accessed before migrating to the Cloud. The associated Cloud risks include SLA breaches, loss of control, data security & privacy, adequately assess risks of a Cloud provider, virtualisation-related risks, compliance risks, decreased reliability since service providers may go out of business, and among others (Fitó & Guitart Fernández, 2010). Usually, people are more comfortable with handling risks they can control. It gives users options to choose from, set priorities, and to act decisively in the best interest of the organisation when an incident happens. Cloud-based services, however, eliminate this, as the processes, infrastructure, and data are beyond the user's control. It makes risk assessment and management a challenging task to achieve as it is not feasible to confirm that the system is functioning as it should nor validate effective security controls are in place (Jansen, 2011, pp. 2-3).

Most solutions for risk management in the Cloud are not all-encompassing, and the responsibilities have been delegated to a trusted third party or CSPs eliminating the consumers in the risk assessment process (Alosaimi & Alnuem, 2016, p. 3). However, risk management should be based on the daily interactions between Cloud consumers and providers, as well as between Cloud providers (Fitó & Guitart Fernández, 2010, p. 2). For Cloud consumers to enjoy the optimum benefits of Cloud computing, the associated Cloud risks must be addressed.

2.8 CONCLUSION

In conclusion, Chapter two has provided definitions of Cloud computing. It discusses centralised and decentralised systems, as well as the re-centralisation of Cloud computing. It provides an overview of the challenges involved with Cloud adoption. It also presents the theories that relate to the adoption of Cloud from the individual and the organisation's perspective, and the researcher's theoretical framework. Chapter three is concerned with the methodology and guidelines used to determine the factors affecting the changing IT security skills and roles in a Cloud-based organisation.

Chapter Three

Research Methodology

3.0 INTRODUCTION

Chapter two has reviewed relevant and related literature for the theme of this thesis. It concluded by assessing the predominant issues and problems arising from the impact of Cloud computing opportunities on organisations. One of the main issues is the impact of Cloud computing on skills and roles in the organisation (Section 2.6). In this Chapter, the issues and problems are to be taken to select one that is feasible to research. Once decided the relevant research questions have to be derived and a methodology set out to answer the questions. The nature of IT and IS research requires adopting a flexible research process to enable iteration among processes and to facilitate the management of the research project (Steenkamp & McCord, 2007).

There has been a shift towards the interpretive case study approach in information system research (Parker, Wafula, Swatman, & Swatman, 1994, p. 202). Interpretive research aims to develop context-based generalisation from the phenomena being studied (Myers, 2019, p. 48). The Case study method is one of the most popular methodologies used in IS research (Shakir, 2002, p. 192). A case study can be used for both descriptive and exploratory research. It is usually informed by the overall research purpose, which may be to explain, explore, describe, or compare cases (Stjelja, 2013). A case study can also be used for theory building or testing (Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Yin, 2009; Ridder, 2017). Most case study research is used for building or modifying theory and is interpretive in nature. Here a researcher is interested in systematically identifying concepts and patterns from data for building theory or expanding existing theory (Bhattacharjee, 2012). The overall study purpose usually guides the selection of a specific type of case study. Accordingly, this study employs an interpretive case study approach.

Chapter three is structured to present the methods and approaches that are used to guide the investigation, as well as a feasibility analysis of the problems identified from Chapter two. Section 3.1 introduces a review of previous studies to identify the

way others have done this type of research. In Section 3.2, the research questions are derived from Chapter two. Section 3.3 discuss the philosophical elements of research, and Section 3.4 presents various research paradigms used in qualitative studies. The justification for selecting the interpretive paradigm is made in Section 3.5. In Section 3.6 the research approach is discussed and research method for the study is discussed in Section 3.7. In Section 3.8, the case description is given defines the research methods for the case study and Section 3.9 presents the research design and the step by step research process was presented in Section 3.10. Section 3.11 defines the theoretical data requirements for the case study, and Section 3.12 the specific data collection steps. Section 3.13 gives the settings of the NVIVO requirements for data analysis and the steps taken for analysing the secondary data. Section 3.14 outlines the limitations of the research methodology, and Section 3.15 concludes the Chapter with a link to Chapter four that reports the findings.

3.1 A REVIEW OF PREVIOUS STUDIES

A review of previous studies is undertaken in this Chapter to identify how the researchers did their research. In Chapter two, papers are reviewed to learn content for the proposed area for study. In Chapter three several papers are reviewed to look at the methods and ways of doing research in this area. First, four studies are reviewed to establish general guidance (Section 3.1.1), and then four studies are evaluated in-depth to identify the research methods used (Sections 3.1.2 -3.1.5).

3.1.1 Four Similar Studies

Jackson (2014) examines the barriers and impact of Cloud computing adoption. A single case study methodology is adopted to capture real-life events. The data for this study is collected through interviews with 11 IT professionals from two different sectors. The participants are selected based on their job titles and decision-making authority. The researcher uses the constant comparative method of moving through developing themes by identifying the differences and similarities between the data until meaningful data is recovered by constant comparison in the multiple data sets. Once the analysis is complete, member checking sessions with participants to improve the accuracy and credibility of the data is added. The data also shows that the participants

are not so convinced that Cloud computing had significant IT cost reduction capabilities. It suggests that a cost-benefit analysis should be used to analyse Cloud computing's true cost savings that should include all costs after the transition to Cloud computing and must be compared with traditional IT-related costs. Additionally, the data also suggests that organisations should set internal goals before transitioning to the Cloud to ensure the right expectations are being set and met. Regarding data security and standardization, it implies that organisations should develop standards to reduce the risk of data security breaches. Furthermore, outsourcing barriers can be overcome through a thorough evaluation of the outsourcer's capabilities before executing a contract. The researcher acknowledges the influence of bias of participants and the small sample size as the limitation of this study.

Similarly, Heublein (2012) conducts a single case study on how organisational ambidexterity is shaped by disruptive innovation in an open-source software provider. The case under investigation is the RedHat company. The RedHat company enterprise provides open source solutions, including high-performing Linux, Cloud, container, and Kubernetes technologies. This study includes three sets of data. First, a three-year survey data on existing employee-related to culture, values, and employee engagement of the RedHat company. Secondly, a semi-structured interview with key senior personnel who have experience with Red Hat Cloud initiatives. The interview is based on determining the degree of ambidexterity present, before and after the Cloud in Red Hat adoption. Finally, a management behaviour survey is used for understanding the level of social support and performance. The researcher used a comparative analysis method, and a structural coding scheme is developed based on the constructs from the data. The case study confirms that the Cloud is both a threat and an opportunity for the company. An opportunity because Red Hat is built on concept openness that prevents vendor lock-in, and this naturally aligns with Cloud environments. Cloud can be viewed as a threat because most of Red Hat's revenue is generated from an on-premise environment such as the Red Hat Enterprise Linux. The demand for such solutions is gradually reducing as public Clouds are being deployed. Also, there's the possibility of disintermediation by Cloud providers. The data also indicates that there is high-level contextual ambidexterity in Red Hat's response. However, the findings of this study

cannot be generalised easily as the perspective may vary in different organisation's cultures. Also, the level of disruption considered in this study might only be applicable to large organisations, and inaccurate to rate the ambidextrous response from Red Hat as Cloud innovations that are still in their early stage. Additionally, the subjective data are from an executive and organisational perspective.

Another study by (Wood, 2017) used mixed multiple case studies to explore the required skill sets of information technology workers in managed hosting environments in higher education. The focus of the study was on institutions that use Blackboard as their learning management system. The researcher adopted a quantitative and qualitative data collection method. For the quantitative phase, data was collected from 28 participants across 25 institutions. The qualitative data was collected from five expert interviews. The researcher adopted a multiple case study in order to understand the situation in great depth for determining similarities and differences of using Blackboard across several institutions. The researcher used pattern matching and cross-case analysis technique to analyse the qualitative data and an analysis of variance (ANOVA) was used to determine if there were significant differences present between employee levels for the quantitative data. Each of the data collected brought a different perspective to the research question. The quantitative data suggested participants did not find that managed hosting environments required additional skills, different staffing models, or additional career trajectories while the qualitative data managed hosting for IT applications place an emphasis on soft skills and increased user communication. Overall, the result suggested that managed hosting for IT applications changes the responsibilities of IT staff, however, the overall impact of a managed hosting strategy on a general workforce is largely dependent on the leadership and the organisational culture of the institution.

A more recent study by Herrod (2018) focused on a single qualitative case study to explore the educational needs of the information security community. The study aimed to identify the current knowledge and skills gap in the information security undergraduate curriculum designed by the National Security Association (NSA) and the Department of Homeland Security (DHS). Data is collected through 12 information security industry experts to establish the knowledge, skills, and abilities of information

security undergraduates in meeting the needs of the information security business community. It is done using three rounds of web-based questionnaires. The data is analysed using descriptive, interpretive data analysis. The data are evaluated and reevaluated throughout three rounds of surveys. The findings indicate that the current curriculum knowledge does not align with the perception and expectation of information security industry leaders. The study recommends re-evaluating the current IS curriculum and teaching techniques to determine the changes that are important to meet the industry requirements. Also, it suggests that industries should take a pro-active approach in working with the National Centers of Academic Excellence (CAE) program to assist in determining the required IS skills and abilities, as well as aligning the objectives to meet the industry expectation.

One of the limitations of these studies is the lack of representation and generalisation of the results. Although case study research has been widely adopted, it is still a subject of argument in the scientific community. The status of the case study method as a valid method in the field of IS is still being challenged because it lacks rigour, and therefore it cannot be readily generalised (Tsang, 2014). There are also claims that the case study has the least attention and support because there is no well-defined protocol (Krusenvik, 2016, p. 1). Pereira (2013) also adds that a known limitation of the case study is the tendency of researchers trying to solve many problems in a single case (Pereira, Almeida, & da Silva, 2013). However, it has been argued that case study results generalisation is analytical, not statistical so that it cannot inappropriately contribute to a theory (Thomas, 2015). The case study method needs to be generalised to contribute to theory; however, this can only be possible if the case study has been appropriately informed by theory during the design (Pereira et al., 2013, p. 153).

3.1.2 PhD on Cloud Outsourcing Impacts

Asatiani (2016) investigated the relationship between Cloud technologies and business impacts in a PhD thesis entitled “Impact of Cloud Computing on Business Processing Outsourcing”. This publication is relevant because it focuses on the relationship between the Cloud adoption opportunity and business organisational effects. It also targeted a specific skill group – business accountants, within the organisation as a case

study. The assertion is that there is a gap in understanding of the Cloud phenomena and the business process effects. The thesis explores the assertion and shows how to undertake such a study. The conclusion shows that there are observable and measurable effects when Cloud is introduced into a business. These impacts are structural and relational and may not occur immediately. The author chose the case study methodology as the relevant methodology for research because of the nature of the phenomena and the complexity of the inter-relationships between variables.

The presentation of the data gathered is interesting. The author chose to use four essays as a descriptive elaboration of the observations and then to evaluate the outcomes. Central to the research is the contention that there is a gap in understanding of the Cloud phenomena and the business process effects, and also a triangulated conception of service, client, and Cloud-based information system. The identification of these objects helps structure a research context. They permitted the collection of useful data and then the storytelling in the form of essays. The first essay provided an understanding of the factors influencing Cloud services adoption. The second and third essays addressed decision-making in the Cloud context and patterns of organisational behaviour. The fourth essay expresses the relationships and observed changes in professional conduct. This third essay and report are particularly relevant to the proposed research. The Cloud service opportunities have the effect of forming external business relationships in new ways but also these new relationships push back on internal relationships and the way business is conducted.

The fourth essay shows that the internal business structures and processes became effected by the new opportunity to interface with clients through the Cloud information system. The methodology is described as interpretative as the author argued that most of what is observed in this type of research is perceptions of reality. The implication is that in these contexts of change often no one has a firm grasp on what is happening or what the future may look like. Hence, perceptions of perceptions become the currency of exchange and that reality is a shifting and evolving concept that never stays fixed in any one place. The situation is a learning context where trial and error are occurring, and evaluation is done on the fly by professionals. The abstraction to the methodology is a tension between positivist and interpretive views of

approaching research. The positive way is to have fixed realities whereas the interpretative way is to have emerging and changing realities. These explanations are helpful in understanding methodological solutions for researching Cloud impacts on business relationships.

3.1.3 SAAS Impacts on IT Department

Winkler et al. (2011) took the topic of software as a service (SaaS) implementation from the perspective of impacts on an IT support department. The challenge for the IT department is to adapt by restructuring roles and skills to the new information management requirements. The research hypothesised that the relationships between the IT department and the business are largely unknown when the changes occur. Also, the arrangements between business and IT departments change, requiring alteration to roles and skill groups. To investigate the relationships interviews are undertaken in four independent case studies. Contingency theory is used to frame the study and to ground assertions in a coherent sequence of evolving scenarios. The net effect of the methodology is to substantiate insight into Cloud impacts at the organisation level. This included governance features, change management requirements, role impacts, and evolving skill requirements.

Three relevant questions are selected to tease out and collect evidence within the contingency perspective. This is a qualitative approach based on interview data from four cases. Semi-structured interviews are used with business and IT representatives of the four companies, to collect data. Reflexive thematic analysis to construct the hypothesis as the research progressed. This is in addition to the chosen guiding theory and added value by engaging the research with its context. Factors are extracted to frame the evolving business – IT arrangements, and to provide explanatory power for the assertion of any given or discovered arrangement. The four adoption case studies are then written for comparative analysis.

The value of this study to the proposed research is in the use of case study and the innovation to mix data collection methods to improve the power of the explanatory framework. This suggests that blindly taking a single theory such as Contingency Theory is insufficient if a meaningful study is to be completed. They also use comparative case study methods. To do four case studies requires substantial resources

in terms of time and contacts, but it provides a comprehensive basis from which to test and develop new theories. The relevance of this study is that it is in the Cloud context. The researchers approached a similar problem to what is found in Chapter two, and have shown a successful way to do the fieldwork.

3.1.4 Cloud Impacts on IT Services

Bharadwaj and Lal (2012) explored the impact of Cloud computing adoption in businesses from the business client perspective. Their first observation is the turbulence caused in the business environment by Cloud services adoption. This is framed as a challenge for survival for all organisations, and a learning curve for all those involved. Terms such as flexibility are used to describe the necessary changes through which an organisation could adapt to the new environment created by outsourced service opportunities. Cloud computing changed the manner in which IT services are delivered to a client and the resource requirements. The impact of this is on the retention of roles and skills to support customer services. The extent to which the customer is now self-driven and independent of the supplier has changed the scope of some roles but increased customer support skill requirements.

The research adopted a case study approach so that knowledge could be obtained from the dynamic and changing business context. Bharadwaj and Lal (2012) mention many times the rate of change and the difficulty of focusing on one or a single variable. Such a focus would be at the expense of the dynamic and evolving complex situation in which the sought after knowledge is embedded. The aim of the research is to understand the Cloud computing adoption drivers and the impact on the organisation. Consequently, the case study is formed from ten IT professionals from different organisations of various sectors. This is an interesting and useful contribution to methodology as a case study is usually of an organisation rather than a professional business group. The results, however, identifies adoption factors and the cascading chain of events leading to organisational change or impacts.

The convenience sampling method is used to get the case participants. Trade magazines are used to identify companies using Cloud services, and upper tier IT management professionals from various sectors having 15-20 years of experience in organisations, targeted. A total of 25 IT professionals from 25 different companies are

contacted through email, and 10 participated. Data is collected through face-to-face, telephone, and Skype interviews. This provides an opportunity to clarify scripts and to definition of a case study, and also the data collection methods. In addition, ethics approval would be required for this type of data collection.

3.1.5 Cloud Impact on University IT Department

Culley and Panteli (2015) investigated the impact of Cloud Computing on a University IT department. They observed the disparity of policy and practice where Cloud computing is mandated as the primary technology platform within the institute, but that the role of the IT department had not been defined. Similarly, a change management plan for the transition is absent. The research shows leadership intention to adopt Cloud services but little understanding of how that might occur or the potential impacts on the IT department. The Cloud Computing proposal can offer the IT department renewed focus and capacity to take on the future requirements, but it has to adapt to a new role. The deliverable from the study is an Information Systems (IS) capability framework to fill the missing information gap. The framework offered a target set of capabilities for the IT department to plot a course into developing the capabilities required to fulfil its changing role within the organisation. It reflected the impact of Cloud computing on the IT department, the IT staff, the skills, and the roles.

The data is collected from interviews. There are 27 semi-structured interviews with people at different levels in the organisation. Among these 15 participants are from the IT department and the others ranged from senior academics and heads of departments to senior staff from professional services. An interview guide is created based on the research questions, to ensure the same information is gathered from each participant. The selection criteria for the interview candidates are determined by satisfying at least three of the following criteria: have some subject matter competence or expertise in IT; be representative of the different management layers of the institute (to mitigate the risk of bias); have some understanding of the strategic value of IT to the institution, and be a stakeholder of IT services, ie. someone that depends on the service.

The data analysis is completed using NVIVO. This is a tool to do thematic coding and to find key phrases in the data that relates to the research questions. What did the

data tell about the role of the IT department and the Cloud impact? The data is coded along with the themes of the Cloud, and cross-referenced with the units of analysis. This study is useful to the proposed study because it is looking at a similar problem but in a single organisation. The data analysis tool NVIVO is also helpful because it shows how the thematic analysis proceeds and what can be expected as outputs.

3.2 RESEARCH QUESTION

To inform the study, a literature review is conducted to find out the current issues of adopting Cloud computing technology. Section 2.7 outlines and discuss these issues and challenges. This analysis aims to identify researchable problems from the reviewed issues and discussion in Section 2.7. A research problem can be defined as a general issue, concern, or controversy that is to be addressed in research (Ellis & Levy, 2008). Ellis and Levy (2008, p. 22) further reveals that a research problem should be active, and does not have sufficient existing solutions. A research problem must not be driven solely by personal experience or observations (Ebberts et al., 2016) as the ability to precisely identify the research problem is the key to having good research. Additionally, Huller et al. (2001) note that a good research question is characterised by the FINER – (Feasible, Interesting, Novel, Ethical, and Relevant) criteria. Table 3.1 shows the FINER criteria for selecting a good research problem.

Table 3.1: Criteria for Selecting A Research Problem
(Adapted (Hulley et al., 2001, p. 20)

Criteria	Description
Feasible	<p>This involves checking the practical limits of research in terms of cost, time, expertise, and scope.</p> <ul style="list-style-type: none"> • Is there an adequate number of subjects? • Is there adequate technical expertise? • Is it affordable in time and money? • Is it manageable in scope?
Interesting	The research area is active, and the answer intrigues the investigator and other researchers.
Novel	<p>This entails ensuring the originality of the research.</p> <ul style="list-style-type: none"> • Does it confirm, refute or, extend previous findings? • Does it provide new findings?

Ethical	It does not pose an unacceptable risk and does not violate any form of ethics. <ul style="list-style-type: none"> • Will the institutional review board approve it?
Relevant	Evaluating the importance of the research area. <ul style="list-style-type: none"> • Is it relevant to scientific knowledge? • Is it relevant to future research?
Research Gap	There is a notable research gap in the literature or the literature does not provide an adequate solution.

A researchable problem usually relates to a specific area while a research question provides specific questions that provide focus on the research problem. A research question is essentially a hypothesis asked in the form of a question (Prasad, Rao, & Rehani, 2001, p. 6) while a hypothesis is “an explanation, tentative and unsure of itself, for specific phenomena about which you have questions” (Prasad et al., 2001, p. 30). A hypothesis is testable and can be falsified or confirmed. Based on the literature review from Section 2.7 and Section 3.1, the following research problems have been identified:

- Trust, data security, and user privacy.
- The disparity in governance, compliance, and regulations.
- Risk management
- Employment and downsizing
- Changes in IT security skills and roles.

Security and privacy issues remain one of the greatest concerns of Cloud users. Up until now, there are still issues around maintaining data security and user privacy. Cloud users need to trust the CSPs provides the necessary security measures. Nevertheless, a considerable amount of work has been done both in the academic and industry worlds to proffer solutions to data security and privacy concerns (Arora, Raja, & Bahl, 2018; Qiu, Gai, Thuraisingham, Tao, & Zhao, 2018; Rawal, Vijayakumar, Manogaran, Varatharajan, & Chilamkurti, 2018; Stergiou, Psannis, Kim, & Gupta, 2018).

Secondly, the issue of disparity in governance, compliance, and regulations is a critical issue that needs to be addressed. The Governance and compliance issue is one of the topmost concern Cloud users have after security threats (Brown, 2019, p. 1). IT governance is important for effective alignment of IT and corporate strategy (Brandis, Dzombeta, Colomo-Palacios, & Stantchev, 2019, p. 1). Compliance is a complex issue in Cloud computing because of the Cloud settings in terms of data storage (van de Weerd, Mangula, & Brinkkemper, 2016, p. 923). Data are stored in different datacenters across different geographical locations across the globe and in different jurisdictions. Organisations face conflicting compliance requirements with CSPs in meeting government and industry regulations. Effective governance, risk, and compliance are important in securing organisation resources when adopting Cloud computing.

Thirdly, there is the issue of trust and risk management. This is because users have no control over their data and it is more difficult to handle a risk that cannot be controlled. Jansen (2011) reveals that it is not feasible to confirm that the system's functionality nor validated and effective security controls are in place. Cloud increases the risks and attack surface for consumers. Risk management is crucial to fully utilising the benefits of Cloud computing. Furthermore, identifying the risks before adopting Cloud computing allows the risks to be managed. Many works are currently focused on risk management in the Cloud.

Fourthly, the review reveals the impact of Cloud regarding skills and roles transformation. The implication Cloud has on the IT workforce especially the IT security workforce has been a point of concern to many. Cloud environments are threatening the relevance of existing IT security jobs by changing their job roles. Cloud is generally changing the IT department from IT service and resource provisioning to overseeing the procurement and delivery of technology by vendors. Unfortunately, little work has been done on exploring the impact of Cloud computing on knowledge and skills (Cloud and the changing roles within IT). Cloud is also introducing new jobs that require new skills and bring about the merging of existing IT jobs while others might become obsolete. The changes might be large since the Cloud is still rather new, and it takes time for the organisational impacts to be felt. IT professionals now must

manage the organisation's technical issues as well as be more business-driven. Currently, the existing IT roles remain the same while their functions are being redefined. The core issues arising from changing IT roles that need answers include: which traditional IT roles should be redefined, re-distributed, and/or made redundant. As of now, there is uncertainty as to whether some roles have fully transformed into Cloud roles or in-between. For example, the role of a Cloud Engineer is responsible for implementing and managing Cloud service delivery models. This role is similar to the role of a traditional network engineer or network/system administrator. However, in a traditional role, the network or system engineer is concerned with designing and connecting the organisation's multiple units across many locations. A Cloud engineer, on the other hand, needs to consider connecting various Cloud services with the backend organisation's network, agility, and disaster recovery. Another similar example is the shifting role of a CIO. The CIO's job role is changing from the technology overseer to managing data as a company's asset (Fisher, 2014, p. 3)

Lastly, Cloud computing technology is causing a significant impact on employment and downsizing. Workers are being faced with the hard choice of having to learn new skills or become redundant or lose a job. This is because some roles are migrated to the Cloud. The evolution of IT security roles and skillsets also increases the likelihood of downsizing current employees and hiring new workers with the required skills. Currently, the existing IT roles remain the same while their functions are being redefined. The core issues arising from changing IT roles that need answers include: which traditional IT security roles should be redefined, re-distributed, and/or made redundant?

While all these issues are of great importance to organisations to get the benefits of Cloud, an important question to evaluate before undertaking a study is to evaluate the interest and feasibility of such an undertaking. The issue of the impact of the Cloud on IT security skills and roles is of particular interest especially since there is not much work in academia in this area. There's been a considerable amount of work from the industry regarding how this change impacts IT workers. However, academia seems to be behind on how these changes impact and how they prepare graduates for the workforce in the changing times.

Organisational leaders need to understand how to effectively manage these changes. Therefore, the purpose of this study is to explore the impact of Cloud in terms of knowledge, skills, learning expectations and the expected IT role evolution. It provides results that help to understand the new IT security roles, the skills required, and the changes that must be made to current roles and knowledge requirements. This framework contributes to the body of literature and serves as a guide to industries that want to successfully implement Cloud. It improves the explanation of the IT security service requirements, and better scope the Cloud impacts for business decision making. To this end, the following research questions have been derived from the literature and the identified emerging issues. The proposed study is aimed to answer the question “what are the impacts of Cloud computing on IT security skills and roles?” The following are the research questions:

- i. What are the IT security skills required by the user organisations for the Cloud environment?
- ii. What are the new and evolving roles for IT security professionals for supporting Cloud computing in user organisations?
- iii. What are the challenges and limitations of the existing IT security skills from the organisation’s perspective when confronted by Cloud computing?
- iv. How should security skills be taught and what is the role of HEIs in equipping graduates with Cloud skills?

3.3 PHILOSOPHICAL ELEMENTS OF RESEARCH

Every researcher has their perspective and assumptions of what constitutes truth and knowledge. These views guide the way they see themselves, other people, and society at large. These views and beliefs are referred to as a paradigm (Schwandt, 2001). A paradigm is described as a set of assumptions, concepts, values, and practices that constitutes a way of viewing reality for the community that shares them, especially in an intellectual discipline (AHPC, n.d.). It is also described as a “set of interrelated assumptions about the social world, which provides a philosophical and conceptual framework for the organised study of that world” (Filstead, 1979, p. 34). Furthermore, Crotty (1998) claimed the practice of research is based on four main questions:

epistemology (the theory of knowledge that informs the researcher), theoretical perspective (the philosophical viewpoint for providing the research methodology), research methodology (overall strategy or plan that links the methods to outcomes which informs the choice of methods), and research methods (techniques used to acquire, process, and analyse data to answer the research questions) (Crotty, 1998). These four questions present the interrelated levels of the process of research design (Creswell, 2003). Similarly, Scotland (2012) reports that a research paradigm consists of four components: ontology, epistemology, methodology, and methods (Scotland, 2012, p. 9).

It is essential to define some terms to understand the different components of philosophies of various research paradigms. Four terms relate to philosophical research paradigms. These are Ontology, epistemology, axiology, and methodology. Ontology and epistemology are the two main philosophical elements that are used in the differentiation of the different types of research paradigms. However, axiology and methodology affect the way research is being investigated (Wahyuni, 2012). The following Sub-Sections define the four terms relating to research paradigms.

3.3.1 Ontology

Ontology is the study of being (Crotty, 1998, p. 10). It explores the question of what makes reality. Ontology defines the researcher's beliefs about the nature of reality. A researcher's beliefs about what is real determine what can be known about reality (Killam, 2013, p. 7). Ontology is an area of philosophy that is concerned with what exists and describes what needs to be done in research. There are generally two broad views of ontology: realism and nominalism (Lawrence Neuman, 2014). The realist belief that the world exists in a pre-organised category is waiting to be discovered. Independently of humans and their interpretations of it. The nominalist beliefs that reality is dependent on social actors and their interpretation because individuals contribute to social phenomena and influence how reality is seen and experienced. They believe that people do not experience the real-world, rather people's biography and cultural worldview are always organising their experiences into categories and patterns (Lawrence Neuman, 2014, p. 94). The ontological assumptions hold that what is believed can exist and are crucial in helping the researcher because it aligns their beliefs

to the research problem and identifies its significance. Also, it allows the researcher to construct meaning from the data that has been collected (Kivunja & Kuyini, 2017, p. 27)

3.3.2 Epistemology

It is the study that explores the nature of knowledge and the relationship between the would-be knower and what can be known (Guba & Lincoln, 1994, p. 108). It is concerned with how knowledge is created, acquired, and communicated (Scotland, 2012, p. 9). Epistemology is derived from two Greek words *episteme*, meaning knowledge, and *epistanai*, meaning to know. It examines the relationship between knowledge and the researcher during the inquiry. The researcher's ontological assumptions usually determine the epistemology (Killam, 2013, p. 8). Wahyuni (2012) notes that epistemology is the overall process of generating and understanding acceptable and valid knowledge (Wahyuni, 2012, p. 69). Epistemological questions such as how do we know what we know? It helps the researchers position themselves in the research context by discovering what is new from what is already known (Kivunja & Kuyini, 2017, p. 27). Epistemology is critical. After all, it affects the whole purpose of research because it defines how the researcher discovers or produces knowledge.

3.3.3 Axiology

Axiology originates from the Greek word *axios*, which means value. It is the study that explores the values of an individual or group (Vaishnavi and Kuechler 2008 p.16). Axiology defines the researcher's values and ethical behavior in conducting research (Killam, 2013, p. 6). It involves defining, evaluating, and understanding the notion of right and wrong behaviours as it relates to research been studies. The researcher needs to consider the privacy, accuracy, property, and accessibility principles for data and all the participants of the research (Kivunja & Kuyini, 2017, p. 28). According to Creswell (2013), the axiology assumption in qualitative research involves the researcher acknowledging the laid down values as well as their values and biases during the research.

3.3.4 Methodology

Methodology refers to the overall strategy used to seek the truth. It answers the why, what, from where, when, and how data is collected and analysed (Guba & Lincoln, 1994, p. 108). It is the process where the researcher finds out what they believe can be known. The methodology is driven by ontological and epistemology beliefs. It involves techniques of systematically discovering knowledge (Killam, 2013, p. 9). The research methodology is not only concerned about what questions are asked but also the overall process of answering the questions and producing a valid result. The overall research process combines ontology, epistemology, and axiology. It demonstrates the process of how a researcher sees, thinks, and acts on the truth.

These philosophical elements altogether constitute the theory or paradigm upon which research is based. Paradigms are the lens upon which a researcher determines what to study and which methods are suitable to use for collecting and analysing data. Also, it determines how meanings are constructed from the data. Paradigms are, therefore, important because they define a researcher's philosophical orientation, which impacts every decision made in the research process (Kivunja & Kuyini, 2017, p. 26).

3.4 RESEARCH PARADIGMS

Research paradigms are “commitments, beliefs, values, methods, outlooks, and so forth shared across a discipline” (Schwandt, 2001, p. 183). It includes assumptions, questions to be asked, and research techniques used in answering the questions (Lawrence Neuman, 2014, p. 96). Paradigm is widely used across various disciplines. However, before the ever-increasing use of the word paradigm, it was first used by Kuhn (1962). He described it as a set of preconceptions from which humans perceive the world. Schwandt (2001) defined paradigm as a shared world view that represents the beliefs and values in discipline and that guides how problems are solved. A paradigm can help clarify research questions and help in research design. Creswell identified three elements involved in research design as the researcher's knowledge claims and theoretical perspective, the strategies of inquiry, and the methods of collecting and analysing data (Creswell, 2003, p. 5).

Each research paradigm is based on ontological and epistemological assumptions. These assumptions guide a researcher to choose the research method and methodology for a particular study (Scotland, 2012). Several types of research paradigms have been identified across various fields. Creswell (2003) identified four paradigm assumptions for qualitative research as post-positivism, constructivism/interpretivism, transformative, and pragmatism. In the same way, Guba et al. (1994) claim there are four basic paradigms for qualitative research: positivism, post-positivism, critical theory, and constructivism. Orlikowski and Baroudi (1991), in their view, outline the three categories as positivism, interpretive, and critical realism. Table 3.3 summarizes the widely used paradigms according to their philosophical elements. The next Section describes four of the widely used research paradigms in IS research.

3.4.1 Positivism

This approach holds that science is the only way to true knowledge and that scientific methods, techniques, and procedures offer the best framework for investigating the social world (Chilisa & Kawulich, 2012, p. 7). The positivist paradigm emerged in the 19th century by Auguste Comte's criticism of metaphysics and assertion that only scientific knowledge can reveal absolute truth (Kaboub, 2008). A positivist researcher believes knowledge is only about what can be observed and measured. The ontology assumption of a positivist is realism, meaning reality exists independently of the researcher, while the epistemology assumption is based on objectivism, and the researcher believes in absolute knowledge about objective reality. Axiologically, the researcher is value-driven and maintains a separation from the research by adhering strictly to the laid down ethics (Wahyuni, 2012, p. 71).

Positivist believes knowledge is absolute and value-free. Their statements are usually descriptive and factual (Scotland, 2012). They argue that the truth is made up of unchanging laws and rules of causations and that there exist complexities that can be overcome by reductionism (Aliyu, Bello, Kasim, & Martin, 2014, p. 81). A researcher can be prevented from influencing the outcome of the research from bias and values by following the prescribed procedures, and the findings should be replicable (Guba & Lincoln, 1994, p. 110). A positivist paradigm approach is aimed at

theory testing, explaining relationships thereby formulating laws producing a basis for predictions and generalisation (Bhattacharjee, 2012, p. 93; Scotland, 2012, p. 10).

3.4.2 Post-positivism

Post-positivism emerged in the 20th century from the criticism of positivism assumptions (Ponterotto, 2005; Scotland, 2012). It is based on critical realism ontology, dualist / objectivist epistemology, and experimental methodology. A post-positivist holds that reality exists but is impartially apprehensible (Guba & Lincoln, 1994, p. 110). That is because the human knowledge mechanism is flawed, and phenomena are intractable. Humans are only capable of knowing reality with some certainty. Similarly, Crotty (1998) argued that “no matter how faithfully the scientist adheres to scientific method research, research outcomes are neither totally objective nor unquestionably certain” (Crotty, 1998, p. 40). Post-positivist researchers believe all observation is fallible and has an error, and all theory is revisable (Wang, Duffy, & Haffey, 2007, p. 2).

Post-positivism holds that objectivity is a regulatory ideal and that findings might be replicated but are subjected to falsification. Similar to the positivist paradigm, post-positivist is focused on understanding casual relationships through experimentation and correlation studies for prediction and generalisation (Scotland, 2012, p. 10). Furthermore, both paradigms serve as the primary foundation and anchor for quantitative research (Ponterotto, 2005, p. 129).

3.4.3 Constructivism /Interpretivism

Interpretivism posits that knowledge is subjective, and it is gained through social and cultural construction. Interpretivist beliefs reality is subjective to people’s experiences of the external world; therefore, reality is socially constructed (Thomas, 2010, p. 295). Interpretivism is a contrast to the positivism approach of realism or objectivism. It holds that multiple, valid realities exist which are socially constructed. A Constructivist seeks to understand the world from the way others view it (Walsham, 1995; Ponterotto, 2005; Chilisa & Kawulich, 2012). They believe knowledge is subjective and value-bound. Therefore, the researcher tends to rely on many participants’ views of a situation and as much as possible. The researcher and the participants jointly co-construct

findings from their interactive dialogue and interpretation (Ponterotto, 2005, p. 129). They believe that there are many interpretations of knowledge, but these interpretations contain the scientific knowledge that they seek.

In interpretivism research, the researcher inductively develops a theory or meaning of patterns rather than starting with a theory like a positivist. In doing so, the researcher acknowledges their bias as they interpret their findings, which are usually shaped by their own experiences and background. Walsham (1995) also views interpretivism research as value-free as the research process is guided by the researcher (Walsham, 1995, p. 376). The research questions are usually designed to be as broad as possible so that the participants can construct the meaning of the situation usually from interactions with other persons (Cresswell, 2013, p. 9). The ultimate objective of an interpretive researcher is to interpret other people's views of the world, and the interpretivism paradigm provides the primary foundation for qualitative research methods. Qualitative research is sometimes referred to as interpretive research (Ponterotto, 2005; Cresswell, 2013).

3.4.4 Critical Realism

The critical inquiry paradigm holds a historical realism ontology, a subjectivist epistemology, an axiology that acknowledges historical values, and a dialogic methodology (Guba & Lincoln, 1994, p. 110). Ontologically critical realist asserts that multiple knowledge exists and operates independently of our knowledge of it (Archer, 2016). The Critical realism paradigm asserts that reality and knowledge are both socially constructed and influenced by power relations from within society. Similarly, Crotty (1998) claims that knowledge is constructed rather than just passively noting the laws of nature. Human actions by the researcher can alter reality and the participants being investigated, are interactively linked with their values influencing the output of the study (Guba & Lincoln, 1994). With the transactional nature of inquiry between the researcher (investigator) and the subjects (participants), a dialogue is needed to transform ignorance into informed knowledge. Guba and Lincoln (1994) put it as “transform ignorance and misapprehensions (accepting historically mediated structures as immutable) into informed consciousness (seeing how the structures might be

changed and comprehending the actions required to effect change) ” (Guba & Lincoln, 1994).

3.5 RATIONALE FOR CHOOSING RESEARCH PARADIGM

As discussed in Section 3.4, there are various research paradigms with no generally accepted one; and, each one has its pros and cons. A research paradigm is usually selected based on the research problem. For investigating the impact of Cloud computing on IT security skills and roles in this research, I seek knowledge from individuals and organisations who have been directly influenced by the changes Cloud is posing. The selected organisations have fully migrated to the Cloud and have been affected in one way or the other. This study aims to seek security expert’s opinions on how the Cloud is changing the knowledge and skills required for IT security professionals and thereby changing and re-defining the roles.

Therefore, the underlying assumptions of this research are based on the interpretivist paradigm with the notion that knowledge is gained interactively from human perception and social experience. The interpretive research paradigm views the

Table 3.2: A Review of Relevant Qualitative Research Paradigms
(Adapted from (Chilisa & Kawulich, 2012, p. 6; Patel, 2015))

Philosophical elements	Paradigm			
	Positivist	Post-positivist	Interpretivist or Constructivist	Critical Realism
Ontology	There is only one reality or truth	There is one reality or truth knowable within a probability	There is no single reality or truth. Reality is created by individuals in groups (less realist).	Realities are socially constructed entities that are under constant internal influence.
Epistemology	Knowledge can be measured, and hence the focus is on reliable and	Knowledge is objective and cannot be perfectly achieved but is approachable.	Knowledge is subjective as it is socially constructed and dependent on the human mind	Knowledge is socially constructed and influenced by power

	valid tools to obtain that.			relations from within society
Axiology	Value-free. The inquiry is highly objective, so data is independent of the researcher	Value-free. The research process is highly objective. Though the researcher believes objectivity is regulatory	Research is value-driven and highly subjective. The researcher is part of the inquiry and cannot be separated	Value-laden, the researcher acknowledges their bias by world views, cultural experience, and upbringing.
Methodology	Qualitative, Experimental research, survey research, quantitative and randomized control trials research	Quantitative, which includes experimental, quasi-experimental, correlational, causal-comparative, and survey designs.	Qualitative, Ethnography, Grounded theory, Phenomenological research, Heuristic inquiry, Action Research, Discourse Analysis, etc.	Critical discourse analysis, critical ethnography, action research, ideology critique.

world from a subjective point of view. It seeks an explanation with reference to the participant rather than the objective observer of the action (Ponelis, 2015, p. 537). A positivist approach is an objective, and value-free approach that is driven by laws of cause and effect; and is not suitable for this study because it is driven by scientific evidence, which is based on quantitative methods. Also, generalisation is limited in understanding human and organisational phenomenon (Sandberg, 2005, p. 41).

An interpretive paradigm approach is most suitable for this study because it focuses on explaining a phenomenon through the meaning assigned to it by others, thus providing deeper meanings to reflect different aspects of the research problem. Furthermore, it offers useful ways of understanding the changes in the security skills and roles through participant's opinions, knowledge, and experience.

3.6 RESEARCH APPROACH

Research approaches are plans and the procedures for research, which range from broad assumptions to details of the method that are employed for collecting, analysing, and interpreting data. The selection of a research approach is usually based on the type of

research problem, the philosophical assumptions of the researcher, the research methods, and the procedures of inquiry (Creswell, 2003). Also, a research approach is based on the anticipated data needed to respond to a research question (Williams, 2007). There are three main categories of research approach: quantitative, qualitative, and mixed-mode research. These approaches are not totally discrete from each other; and, they represent different ends of a continuum. The qualitative and quantitative approach has been differentiated in literature with the terms of words or numbers, type of questions (open-ended or closed-ended), deductive, or inductive.

While the fundamental difference of both methodologies has been demonstrated, it is argued that a precise way to view the difference between qualitative and quantitative approaches is not in the methodology, i.e., rather in the researcher's philosophical assumptions (Atieno, 2009; Creswell, 2014). The epistemological and ontological assumptions of a qualitative researcher differ from a quantitative researcher. Both approaches have different ways of viewing the world and data. This approach entails a specific way of thinking about data and using techniques as tools to manipulate data to achieve a goal (Atieno, 2009, pp. 14-15). There are three types of research approaches: quantitative, qualitative, and mixed method. The following Section describes the different types of research approach.

3.6.1. Quantitative Approach

The quantitative approach focuses mainly on quantifying data and control of empirical variables (Ponterotto, 2005, p. 128). This approach uses a large sampling size and statistical analysis to find relationships between data. The quantitative approach is aimed at testing or verifying theories by examining the relationship among variables (Creswell, 2014). The underlying philosophical assumption is that of a positivist. The researcher believes knowledge is objective, replicable, and can be generalised. It usually employs experiments and surveys to collect data. Also, the quantitative approach allows the researcher to have some control over the data collection method, and there is no direct contact with the participants (Eyisi, 2016). The questions are usually closed-ended with a predetermined response. Quantitative researchers focus on numbers and figures; they employ statistical tools for analysis, which is known to save time and resources (Eyisi, 2016, p. 94). The goal of a quantitative study is in describing

and explaining current situations by establishing relationships and ones between variables (Mertler, 2016, p. 108).

3.6.2 Qualitative Approach

The qualitative approach is used for exploring and understanding the meaning of individuals or groups ascribe to a social or human problem (Creswell, 2014). It is particularly useful in simplifying data while retaining its context and complexity (Atieno, 2009). Qualitative research is designed in social sciences fields to study social and cultural phenomena (Myers, 1997). However, today, qualitative research is being used extensively across many fields.

There's also been a rise in its use in the field of Information Systems (Baskerville & Wood-Harper, 1998; Mangan, Lalwani, & Gardner, 2004; Singh & Bartolo, 2005; Matsuo, Wong, & Lai, 2008) due to the shift from technical to managerial and organisational issues (Jabar, Sidi, Selamat, Ghani, & Ibrahim, 2009, p. 47). It uses the constructivists / transformative philosophical assumption. It asserts that knowledge is gained interactively through human experiences. Qualitative research uses methods such as narrative, phenomenological, grounded theory, case study, and ethnography for collecting data (Creswell, 2014). The purpose of qualitative research is to understand the participant's view of a concept or phenomenon. The researcher collaborates with the participants to provide deep insights into the research problem.

3.6.3 Mixed Approach

A mixed approach is a form of inquiry that combines both qualitative and quantitative approaches. It requires a purposeful combination of methods and data integration to allow a comprehensive view of the research (Shorten & Smith, 2017, p. 74). It uses the pragmatism philosophical assumption, which asserts that the best approach or method of inquiry are those that help to answer the research question effectively. This approach provides strengths that outweigh both qualitative and quantitative research by providing a complete and comprehensive of the research problem. The idea behind mixed methods is that both qualitative and quantitative methods have biases and weaknesses, and the collection of both data help neutralise the weakness of each data (Creswell, 2014).

Mixed method research is particularly useful in answering research questions that either quantitative or qualitative approaches cannot sufficiently answer alone. It can provide a better understanding of connections or contradictions between qualitative and quantitative data (Shorten & Smith, 2017). Although the mixed methods can help enrich the evidence of inquiry, it also introduces some level of complexity in conducting research. It requires more resources such as time, and personnel (Shorten & Smith, 2017, p. 75)

3.6.4 Rationale for Choosing Qualitative Research Approach

Given that the primary aim of this study is to understand the impact of Cloud supporting IT security in skills and roles, the study requires a context-based research method that provides deep insight and allows capturing other people's perspectives of real-life situations. A qualitative research approach is best suited for this study. The qualitative research approach is best suited for a study that serves the purpose of description, interpretation, verification, and evaluation of a study (Peshkin, 1993). Also, qualitative research generally seeks to answer the what, how, and why questions rather than how much, or how many (Bricki & Green, 2007). This best suit this study as it is focused on the "what" questions.

Qualitative research is an interpretive-based method that seeks to understand the way others conceptualized events and concepts (Kaplan & Duchon, 1988, p. 572). Creswell (2000) indicates that qualitative research is more concerned with the views of people who conduct, participate in, or read and review a study (Creswell & Miller, 2000). Also, qualitative research tends to focus more on how or what, which enables the researcher to explore in-depth a specific context and observe the situation. Furthermore, Kaplan and Maxwell (1994) observe that when textual data are quantified, the aim of understanding a context from the participant's view is lost. This makes a qualitative approach suitable for exploring opinions and perceptions. Hence, the choice of qualitative research is most appropriate for this study.

3.7 RESEARCH METHOD

A research method refers to specific techniques and procedures for collecting and analysing data (Crotty, 1998, p. 3). As can be seen in Section 3.2 from the review of

previous studies related to the impact of Cloud computing on IT, most of the studies adopted case studies. According to Yin et al. (1994) the criteria for choosing a research method is dependent on “the type of research question posed, the extent of control an investigator has over actual behavioural events, and the degree of focus on contemporary as opposed to historical events”. Different strategies for qualitative research can be illustrated with case study methods, ethnographic method, narrative, phenomenological, and action research methods (Myers, 1997).

Ethnography is a method where the researcher studies a cultural group in a natural setting over a long period of time by collecting, primarily, observational data (Creswell, 2003). Ethnography is originally used in social and cultural anthropology, where ethnographers are required to spend quality time in the field studying people (Myers, 1997). However, ethnography is now widespread in the field of information systems (Orlikowski & Baroudi, 1991; Hughes, Randall, & Shapiro, 1992; Myers, 1999). Ethnography is an in-depth research method as it provides the researcher with a deep understanding of the situation (Myers, 1999, p. 2).

In grounded theory, the researcher focuses on deriving a general, abstract theory of a process. According to Glasser and Strauss (1967), who discovered the grounded theory, described it as an inductive development of theory from data. Grounded theory is particularly interested in theory development. The grounded theory method is becoming popular in IS as it is useful in developing a context-based and process-oriented description of a phenomenon (Myers, 1997).

In phenomenology research, the researcher seeks to understand human experiences concerning a phenomenon from the participant's perspective (Creswell, 2003, p. 15). Phenomenological methods are particularly effective at bringing to individual experiences and perceptions from their view, thereby bringing to the surface deep issues and making it a basis for practical theory (Lester, 1999). Unlike the other methods, case study research allows the researcher to explore and understand complex issues with a focus on contemporary issues. It is useful for exploring, classifying, and developing hypotheses and theories (Benbasat, Goldstein, & Mead, 1987, p. 371).

3.7.1 Case Study Method

Case studies have been extensively used in IS research (Tsang, 2014). The IS field has experienced significant progress concerning interpretive research over the past decades (Fernández, 2004). A case study provides the opportunity to examine a research problem in real-life contexts (Wieringa, 2013, p. 2). Leedy and Ormrod (2014) observe that the purpose of a case study is to examine a person or situation in great depth (Leedy & Ormrod, 2014, p. 258). Also, Cope (2015) reports that a case study is a flexible research as it allows multiple sources of data. Case study research is different from other types of research because it provides an intensive analysis and description of a single unit or system defined by time and space (Hancock & Algozzine, 2017, p. 9). It is beneficial when researching a new or developing research area. As a result, several studies have used a case study method in solving issues related to the adoption of Cloud computing in an organisation.

The case study method has developed over the years and has become an effective approach for investigating and understanding complex real-life issues (Harrison, Birks, Franklin, & Mills, 2017, p. 1). It has evolved across varied disciplines into a more pragmatic and flexible approach (Harrison et al., 2017, p. 2). The case study has multiple definitions. Yin (2009) defined a case study as “an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident” (p. 18). A case study is a detailed study of a single phenomenon from a general category (Myers, 2019). In Creswell’s view, a case study is a method in which the researcher explores in depth a program, an event, an activity, a process, or an individual or group (Creswell, 2003). A case study research is driven by the researcher’s interest rather than the method itself (Hyett, Kenny, & Dickson-Swift, 2014). It is particularly useful when there is a need to answer the "how" or "why" questions and when the studies are focused on a contemporary phenomenon within some real-life (Yin, 1994, p. 1). Yin (2009) identified different methods and a decision matrix to assist in understanding which method to use. Table 3.3 gives a summary of the decision matrix. A case study is a very useful and robust research method when a holistic, in-depth investigation is needed. It

is highly descriptive because it is rich in deep and varied sources of information (Hancock & Algozzine, 2017, p. 16).

Table 3.3: Relevant Situation for Different Research Methods

(Yin, 2009)

Method	Form of research question	Requires behavioural control of events?	Focuses on contemporary events
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, How many, how much?	No	Yes
Archival analysis	Who, what, where, How many, how much?	No	Yes/No
History	How, why?	No	No
Case study	How, why?	No	Yes

3.7.1.1 Types of case study research method

There are different types of case studies that can be considered in a qualitative study. The selection of a specific type of case study is usually guided by design are guided by the overall study purpose. Yin et al. (1994) identified three categories of case study as explanatory, exploratory, or descriptive. He further classified types of case study research design as a single study and multiple case studies. An *explanatory* case study explains the same sets of events and justifies how these explanations are applicable in other situations (Yin, 1994, p. 5). It is useful in explaining casual relations and theory development (Stjelja, 2013, p. 4). An *exploratory* case study is used to explore those situations in which the intervention being evaluated has no clear, single set of outcomes (Yin, 2009; Sepehr & Aghapour, 2012, p. 1). The goal is usually to prove that further investigation is necessary from a case. It is usually very broad and serves as a preliminary step for explanatory case research (Stjelja, 2013, p. 3).

Descriptive case studies are used to describe an intervention or phenomenon in the context in which they occur (Yin, 2003). It is usually focused and detailed; and, it

is used in describing various characteristics of a phenomenon in its context and, therefore, useful for building theory (Stjelja, 2013, p. 4; Baskarada, 2014, p. 4). A *single case study* is used to explore a distinct or unique phenomenon that might have been inaccessible to scientific observation (Yin, 1994, p. 40). It also helps the researcher to test a theory's propositions. *Multiple case studies* enable the researcher to explore differences within and between cases. The goal is to replicate findings across the cases. The findings drawn might predict similarly, i.e., replicate similar results or contrasting results, i.e., replicate a theory (Yin, 1994, p. 46). It is suitable for theory testing, for establishing the generalizability of inferences, and for developing richer interpretations of a phenomenon (Bhattacharjee, 2012, p. 95). *Collective cases* are very similar to multiple cases in their nature. The collective case provides insights into other things rather than the case itself (Stake, 1995; Yin, 2003; Stake, 2005).

Furthermore, Stake classified a case study as intrinsic, instrumental, and collective. In an *intrinsic* case study, the researcher's primary interest is in having a better understanding of the case itself rather than understanding some abstract concept or generic phenomena. In an instrumental case study, the researcher is more concerned with gaining insights into other things rather than the case itself. An *Instrumental* case study is useful in theory refinement (Stake, 1995, p. 3; Stake, 2005). An instrumental case study facilitates understanding something else other than the case. Table 3:4 summarizes the types of case studies.

Table 3.4: Types of A Case Study

Type	Purpose	Theory
Explanatory	Explaining a phenomenon	Building theory
Exploratory	Prove further investigation is needed	Theory building
Descriptive	Examine a case in details	Building theory
Collective or Multiple	Replicate findings across cases	Theory refinement or replication
Single or Intrinsic	For unique and unusual phenomenon	Theory testing or refinement
Instrumental	For case description	Theory refinement

Theory plays an integral part in case study research. The case study research method can be used in different modes for theory testing, theory-building, or modifying an existing theory. Eisenhardt (1989) first conceived the concept of building theory from a case study. She asserts that to capture the richness in observations and prevent the limitations of existing theories; it is better not to consider no theory first during case investigation. Furthermore, while formulating research problems is important, researchers should avoid thinking about specific relationships between variables and theories as much as possible as it may bias and limit the findings (Eisenhardt, 1989, p. 536). Similarly, Dobson (Dobson, 1999) argued that the use of theory could hinder the researcher from seeing other perspectives (Dobson, 1999, p. 261). Qualitative data is usually the choice of data for case study research. Systematic procedures are used to compare the emerging patterns, constructs, and relationships within the data, to eventually lead to a new theory (Ridder, 2017). While the idea of no theory case study might be commendable, it is unrealistic and not feasible as it involves the researcher considering everything about the case (Eisenhardt, 1989, p. 536; Dobson, 1999, p. 262). It is impossible not to bend towards a theoretical orientation while preparing for research questions evaluations, and methods of data collection. The main difference between the two theoretical frameworks is whether the researcher decides to consciously work within it or tries to work outside the framework (Kaplan & Maxwell, 2005, p. 37).

Similarly, Bhattacharjee argued that the construct of a case needs to be known *a priori*; however, the construct of interest may emerge from the data, which means research questions may be modified if found less relevant (Bhattacharjee, 2012, p. 93). According to Yin (2009), the basis for a case study research should be based on a theory. It gives direction to the kind of questions a researcher asks. Furthermore, a case study is used in testing a theory or hypothesis. Testing a theory goes beyond confirming or confuting a hypothesis; it could lead to theory refinement or the development of an alternative theory (Chukwudi, Zhang, & Gable, 2019, p. 3). Riddle suggests that a theory-testing case study research can be used to identify an anomaly in existing theory. The aim of the researcher is not to reject the theory rather to demonstrate the theory is incomplete (Ridder, 2017, p. 289). A case study can also be used to extend or find the

limitations of an existing theory. Ketokivi and Choi (2014) referred to it as theory elaboration. The theory might be elaborated by introducing new concepts or conducting an in-depth relationship between concepts. Several theories can be combined or used by adding new concepts from another theory. Generally, the theory-elaboration case study treats the theory as malleable (Ketokivi & Choi, 2014). Most case study research is used for building or modifying theory is interpretive. The researcher is interested in systematically identifying concepts and patterns from data for the purpose of building theory or expanding existing theory (Bhattacharjee, 2012).

While there are many benefits of using a case study, it is important to note that a case study, like any other, has its limitations. Yin (2009) emphasized that the case study complements the strengths and limitations of other types of research. One of the inherent limitations of a case study from literature is the lack of rigour, and as a result, findings cannot be generalised (Yin, 2009; Pereira et al., 2013; Tsang, 2014; Krusenvik, 2016). Bhattacharjee (2012) also indicates that case study weakness is the issue of internal validity, which is common in other research methods except for experiments (Bhattacharjee, 2012, p. 93). Studies have shown that the criticism against the case study is the very reason for doing a case study. For example, Siggelkow (2007) reveals that the issue of generalisation in a case study might be absurd in some situations and could be a mismatch of method and goal because a case is unique to an individual, group of people, organisation, or event. He advised that a sample should not be chosen randomly but carefully because it would provide information that cannot be necessarily sourced elsewhere. He also notes that small sample size in a case study should not necessarily be a research limitation because a single case can be a compelling example (Siggelkow, 2007, pp. 20-21). More importantly, he reveals the importance of theory, the conceptual framework in improving the reliability of a case study. However, he shows that when making conceptual arguments and analysis, the researcher should be cautious with conclusions made when studying a unique case; they should be more of a persuasive argument close to theoretical constructs (Siggelkow, 2007, p. 23).

3.7.1.2 Rational for choosing case study research

Given the nature of the research questions in Section 3.1 and evidence given in Section 3.6, this study is a qualitative interpretive study. The case study method is considered

most appropriate for this study as it provides behavioural conditions through the actor's perspective (Zainal, 2007, p. 1). Additionally, case studies focus on contemporary events and do not require behavioural control. Furthermore, a case study is very useful in learning and evaluating organisations' complex issues (Baskarada, 2014). While other qualitative methods such as action research, ethnography, and grounded theory are considered, a case study is found to be most suitable for this study. Grounded theory is a widely used qualitative method for explaining change or a process with the overall objective of inductively developing an explanatory theory. While the grounded theory method could be used, the overall goal of this study is not theory generation, rather examine the impact of Cloud computing on IT security skills and roles.

Action research is also well suited for examining change processes in social contexts, but it involves the active and deliberate involvement of the researcher in the context of the study (McKay & Marshall, 2001). The researcher is seen as an active participant and collaborates with other participants relying on each other's skills, experiences, and competencies. Also, Ethnography depends mainly on direct observation and cultural relativism (Padgett, 2017, p. 32), which is not appropriate for this study. It requires a considerably long amount of time to gather data. The aim of the case study is not to intentionally intervene in a situation but rather seek to first understand the case in order to describe it. The overall goal is to use empirical evidence from people in an organisation to make an original contribution (Myers, 2019, p. 90). This fits perfectly into the purpose of this study. Therefore, the case study method has been assessed for this study as it provides in-depth information on the changing IT security skills and roles in Cloud computing.

3.7.1.3 Rationale for case selection

The sampling in the case study is purposive; therefore, while planning the case selection, the first decision is whether the case would be at the individual, group, and organisational level or at multiple levels. A multiple-level case study provides insight into the changes in IT roles and skills from the organisation's perspective. IT professionals from different organisations using Cloud services are interviewed to explore the impact of migration on Cloud computing and related security skills needed. This is suitable for this study as the Cloud domain is still

evolving and a developing area as more organisations move to Cloud or consume Cloud services. Selecting a case at the individual level across different organisations to capture rich data needed for this study as the aim of this study is focused on the changes in individual skills and roles and the overall impact it has on organisations. Interviewing individuals from various organisations who are impacted by cloud computing produces rich data rather than interviewing hiring managers from organisations. Therefore, in this study, a single case method is adopted, and the unit of analysis is the participants.

3.8 THE CASE DESCRIPTION

The goal of this study is to explore the impact of Cloud computing on IT security roles and skills. The intention is to identify the skills and roles that change before and after adopting the Cloud to better equip decision-makers for undergraduates planning to join the workforce as well as organisations planning to adopt Cloud. Cloud is changing how organisations work and IT security workers are impacted. Some of them are being replaced by third-party Cloud-based applications and infrastructures, which do not require the support of internal IT staff. The organisation's Cloud needs' determine the type of Cloud services they adopt which in turn influence decisions about changes to job roles and required skills. While there is a growing concern about possible job loss as the Cloud adoption rate continues to increase, there is limited research in this area. Most of the literature has been focused on the benefits of Cloud computing and how to manage the risks and security issues (Youseff et al., 2008; Armbrust et al., 2010; Bohm et al., 2010; Jadeja & Modi, 2012). This study aims to understand how Cloud is changing IT security jobs and skills required for workers. The case study is appropriate for studying in-depth a distinct situation or phenomenon of interest. It is particularly useful because it offers breadth and diversity in terms of methods of data collection and analytical methods (Adolphus, 2011).

Harrison et al. (2017) listed characteristics of a case study as other research methods, holistic, in-depth study, unit analysis, a case boundary, use of multiple data collection, and analysis methods (Harrison et al., 2017). Table 3.5 lists the core elements of this case study. The case refers to the unit of analysis and it is defined as

an instance of an object of study (Miles & Huberman, 1994, p. 4). The unit of analysis is the major entity that is analysed and it can be social (individuals, a role, a group, community, or other social interactions), temporal, geographical, or artefacts (books, photos, newspapers; technological artefacts) (Fletcher & Plakoyiannaki, 2008, p. 18). Researchers undertaking case studies have the tendencies to study a very broad topic with many objectives. Yin (2003) and Stake (2005) introduced the concept of boundary to know what the case does not include. Research questions help to define the boundaries of the case which manages data collection and analysis limits (Harrison et al., 2017).

The case for this research refers to a person, an IT security professional who is using one or more Cloud services in their organisation. The case selection is chosen to capture the changes of Cloud computing on job roles and skills required by IT security professionals. The case selection is approached from an individual perspective, that is, it focused on variables such as job role, experience, Cloud service, and readiness in New Zealand.

Table 3.5: The Elements of The Case Study

Elements	Description
Objective	To investigate the impact of Cloud computing on IT security roles and skills
The case	IT security professionals using Cloud services
Unit of Analysis	Individual-level (IT security professional employee)
The boundary	In New Zealand with the space of 6 months
Multiple cases of evidence	Interview, Surveys, and documents
Case design	Single case
Analysis	Thematic analysis

All these variables are determined from the literature while deriving the research questions. The participants need to have experienced these changes. In the previous studies reviewed in Section 3.1.4, the researchers adopted a case study approach and then approached 25 IT professionals who fitted the role and sector criteria for an IT Professional. This is a helpful approach because in Cloud the relevant IT professionals are also distributed by Cloud participation rather than a fixed organisation or geographic location. Hence in this research, it is relevant to adopt the Sangeeta & Lai (2012) approach and take the IT professional group to be the case study.

The criterion for the case selection is based on four dimensions: roles, experience, Cloud services, and industry. While a truly representative sample for a case is difficult to achieve, each of these dimensions is varied to answer the research questions within the population of interest through a thorough literature review. To get a reliable and robust result, it is important to capture IT security professionals from these dimensions of experience that are using different Cloud services in New Zealand. The rationale for the case selection is that Cloud computing affects some roles more than others and the level of impact felt is dependent on the level of Cloud services an organisation is using. Cloud is disrupting business structures which are resulting in job displacement and creation. In the short term, the workers whose skills and experience are devalued are likely to lose their jobs, and only highly skilled people are favoured (Commission, 2019, p. 24). The job roles are created by the organisation and are dependent on the size and management of an organisation. The experience is a crucial dimension to this study. Only people who have worked in traditional on-premise work settings and the Cloud environment are in the sample to be studied. This is based on the assumption that Cloud computing has affected them and how they work, and what skills they require to work. Also, the Cloud service dimension specifies the Cloud service used and possible CSPs. This is to highlight any relationship that may exist between the type of Cloud, skills, and roles requirement. Having people from different industries provides a varied perspective on the overall impact.

The case is carried out in New Zealand because of accessibility and the growth rate of Cloud adoption. New Zealand enterprises are experiencing an increase in the adoption of Cloud computing. Several industries including manufacturing, health, IT,

banking, legal, education, and public organisations in New Zealand have adopted one or more Cloud services in the last decade. The IDC reported that New Zealand public Cloud services vendor revenue reached \$1.10 billion in 2018 with Software-as-a-service (SaaS) revenue and infrastructure-as-a-service (IaaS) revenue contributing the largest portion to Cloud services revenue, respectively. Furthermore, there has been a 30.1% growth in public Cloud services since 2017 with the three major providers being Amazon Web Services (AWS), Xero, and Microsoft (Azure) (Gorton, 2019). The penetration rate of Cloud computing in the New Zealand market makes it suitable for this study. It presents a relevant case study and provides access to explore the impact of Cloud computing.

The case design is a single case study. A single case study is chosen as the aim is to study the impact of Cloud computing on a single group of people (IT security professionals) irrespective of their organisations. The participants are technically capable of evaluating the impact of Cloud computing as they have experienced the transition from an on-premise traditional setting to a Cloud-based setting. The unit of analysis is the social unit at the individual level, that is, individual IT security employees rather than the organisational level. As the aim is to capture the new skills requirement and changing roles, the experience of individuals who have worked in a traditional setting and a Cloud environment provides detailed and rich information. The research objectives served as a guide in the selection of the case. As a case study is driven by the researcher's interest and the feasibility of the study, the case selection is driven by purposive sampling, so the case is strategically selected. Also, random sampling is not suitable when the size to be studied is small (Shakir, 2002{Yin, 2003 #232}).

3.9 RESEARCH DESIGN

The research design consists of six phases, as can be seen in Figure 3.1. The research design is adapted from Yin's (2009) case study process: plan, design, prepare, collect, analyse, and report. The first phase is the preparation stage. This phase is concerned with the exploration of literature for problem background and identification. The purpose of this phase is to identify the research gap and formulate research questions

from the problem background through an extensive literature review. The second phase is the design phase. This stage is concerned with the problem feasibility in terms of resources, time, ethics, relevance, expertise, and the scope of the research. It takes a lot of refining of the problem by exploring the literature further. Also, it involves justifying the reason for the study as well as developing theories and choosing the appropriate method for the study.

The third stage focuses on developing the appropriate skills needed for data collection. It involves knowledge and protocol preparation. The knowledge aspect entails understanding the objective, research domain, theory, and methodological issues while the protocol preparation entails understanding the research process and field procedures. The third stage is concerned with the hypothesis and research question formation. Once the research question has been formed, the fourth stage is concerned with identifying a suitable research methodology. This is done through extensive studying of the literature by reviewing the methodology used in similar studies and ensuring the research objective are met through the chosen method.

The fourth stage is the data collection stage. This stage is concerned with the overall techniques and procedures for collecting data for the study. This step also involves exploring the literature for the data collection process in similar studies. Furthermore, the type of data needed to answer the research questions is decided as well as the participants. The fifth stage involves the process involved in preparing the data for analysis and the actual analysis. Data are transcribed, and codes are assigned using the theoretical framework. The last phase of the design includes the proper dissemination of the output of the study. The result of the data analysis is presented in the form of a framework, scholarly publications, and a Thesis.

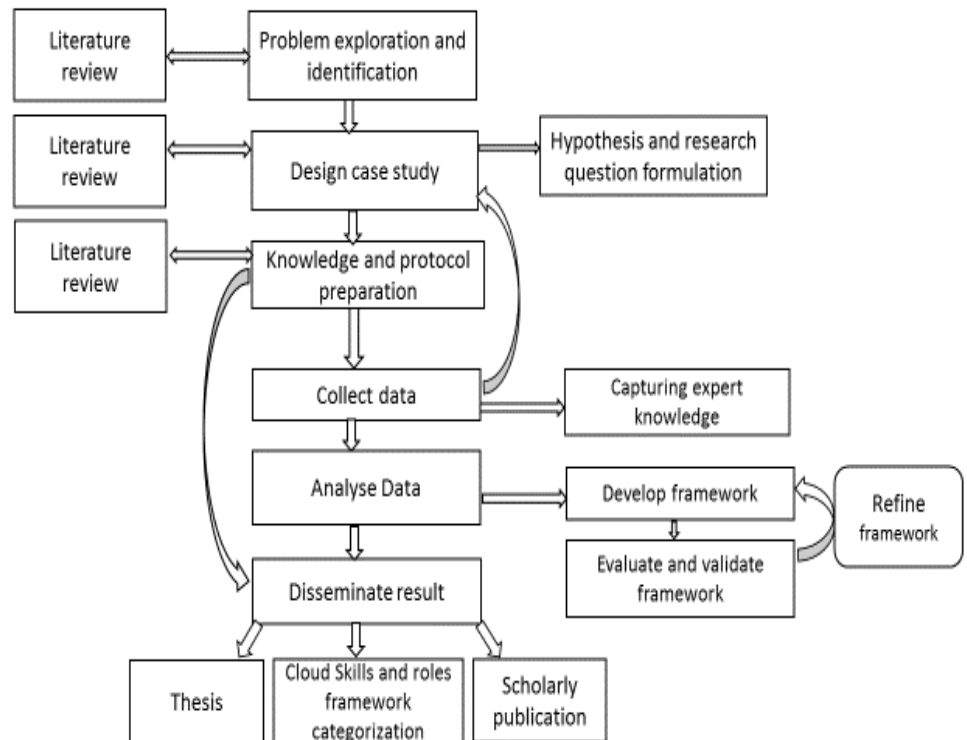


Figure 3.1 Research Design

3.10 RESEARCH PROCESS

This Section describes the step-by-step process of the research design. The first step involves formulating the research question. This step involves exploring the literature for problem background and identification. This is done through brainstorming for research keywords and keyword search selection from the AUT digital library. The second step is to determine which method would be efficient to realise the research questions and objectives identified in step one. This is also done by exploring the literature to examine different methods used in similar studies. The third step is to design the case, interview protocol and survey question. Here the case is selected, and survey and interview questions were designed. Also, this step involves ethics application and approval as well as the selection of proposed respondents and participants.

Furthermore, the curriculum and certifications to be reviewed were concluded. The fourth step is a pilot study. The purpose of the pilot is to test the survey questions to ensure that it captures the data needed for the study. Based on the respondents' feedback and recommendations, the questions were modified, and a second survey question was created. An invitation was sent out to respondents to fill the second survey. The fifth step is the actual data collection using the three data collection methods concluded from step two. The sixth is the data triangulation, all data were reduced to text and managed through Nvivo. The seventh step is the data analysis and is done using NVIVO 12.0. The data was explored and categorised into themes. Finally, step eight presents the findings of the study. Figure 3.1 gives the overall research steps for this study.

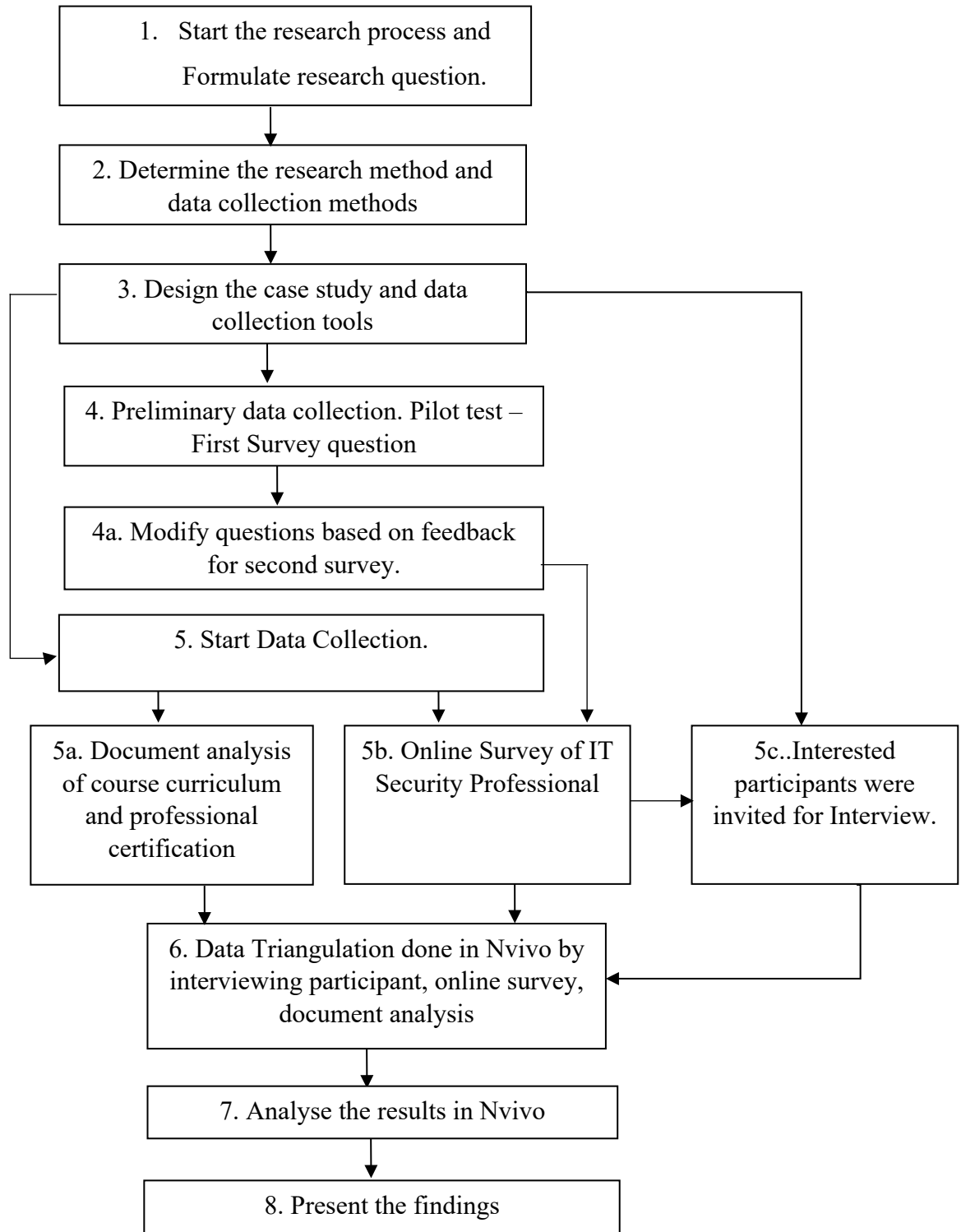


Figure 3.1: Step-By-Step Research Process

3.11 THEORETICAL DATA REQUIREMENTS

This Section explains the method that is employed for collecting data for this study. Given the primary aim of the study is a qualitative approach, qualitative techniques are used. The qualitative approach is best suited for a study that serves the purpose of description, interpretation, verification, and evaluation of a study (Peshkin, 1993). The following Section describes the general approach used for collecting data, data processing, and analyses.

3.11.1 Data Collection

Considering the type and nature of the research method qualitative data are collected. These are the data used in understanding the depth and complexity of a research problem. Qualitative data are often textual such as interview transcripts, field notes, etc. (Hox & Boeije, 2005, p. 593). Generally, qualitative data can be from both primary and secondary sources. Primary data are new data collected for the specific research problem using the appropriate procedures and techniques. They are original data collected by the researcher for their research purpose (O'Reilly & Kiyimba, 2015, p. 85). It usually involves collecting a large amount of data from a small purposive sample using methods such as interviews, surveys, focus groups, or observation (Hox & Boeije, 2005).

Secondary data is the re-use of existing primary data. This is document analysis. Secondary data are particularly useful in generating new scientific and methodological understandings (Irwin, 2013, p. 295). This study is going to employ both primary and secondary data. The primary data is collected through a purposive, semi-structured interview, and a survey. The documentation and critical reflection methods are used for gathering secondary data. The documents include reviewing the undergraduate curriculum from New Zealand universities and professional certification curriculums. These methods have been carefully chosen to capture the data needed for this study.

3.11.1.1 Interview

An interview is a process of asking participants questions, usually in a one-one or group setting (Driscoll, 2011, p. 154). It is a discussion between the researcher and the participant to gather information on specific topics (Harrell & Bradley, 2009, p. 6).

Interviews are particularly useful in doing exploratory and descriptive studies (Mathers, Fox, & Hunn, 1998, p. 1). Also, interview research methods are more powerful tools for obtaining narrative data that allows researchers to investigate people's views in greater depth compared to questionnaires and surveys. Additionally, Harrel & Bradley (2009) reports that interviews provide a complete response because respondent gives a depth of information and also resolves any kind of conflicting information (Harrell & Bradley, 2009, p. 10).

In particular, an expert interview is concerned about the participant's knowledge and experiences as a result of their actions, roles, responsibilities, or obligations within a specific organisation or institution (Littig & Vienna, 2013). An expert interview provides insights into background information, such as expert knowledge and descriptions of processes (Harrell & Bradley, 2009, p. 24). Also, expert interviews are a more efficient and concentrated way of gathering quality data quickly than using observation and surveys (Bogner, Littig, & Wolfgang, 2009, p. 3). An expert in this sense is a person with insight into aggregated or specific knowledge (Van Audenhove, 2007, p. 5). Furthermore, one of the strengths of the Interview methods is that it gives voice to common people, which allows them to present their life situations in their own words freely, and provide personal interaction between the researchers and their subjects (Kvale, 2006, p. 481).

Conducting interviews requires careful planning and developing skills such as intensive listening and developing expertise in the research area (Qu & Dumay, 2011, p. 239). Interviews can be structured, semi-structured, and unstructured (Mathers et al., 1998; Harrell & Bradley, 2009). The types of interviews are categorized based on the level of control the researcher has over the interview process. In structured interviews, the researcher asks the participants the same type of questions in a specified order. The process is strict and highly controlled (Mathers et al., 1998; Harrell & Bradley, 2009). This type of interview asks questions that are usually closed-ended, where the respondents are limited to pre-coded responses (Mathers et al., 1998). Structured interviews are useful when there is a large sample and seeking data that can be generalised (Harrell & Bradley, 2009, p. 28). Semi-structured interview falls in the middle of the continuum of the level of control a researcher has over how questions are

answered. It involves preparing standardized questions consistently and systematically that are guided by broad themes the researcher intends to cover (Harrell & Bradley, 2009, p. 27; Qu & Dumay, 2011, p. 246). The researcher has some level of control in the order the questions are asked. A Semi-structured interview usually makes use of open-ended questions and the researcher can probe the respondent to further elaborate on a response which allows the researcher gain detailed response from the respondent (Mathers et al., 1998, p. 2). The Semi-structure is flexible and accessible and particularly useful in studying human and organisational behaviour (Qu & Dumay, 2011). In an unstructured interview, the researcher has little control over how the respondents answer the questions. Unstructured interviews are based on the notion that the researcher does not know all the necessary questions beforehand (Qu & Dumay, 2011, p. 245). An unstructured interview is sometimes called a depth or in-depth interview. It has no preconceived plan nor anticipation of how the interview proceeds. (Mathers et al., 1998, p. 3). Though unstructured interview may lead to gathering rich information, it is very time consuming and are most suitable when the researcher has a lot of time to spend studying (Harrell & Bradley, 2009).

For this study, data is collected through a purposive, semi-structured, industry-based interview method. This method has been carefully chosen to capture the data required for this study. Stake (2005) adds that sampling for a case study research cannot be random, as it has to be chosen based on the interest of the researcher. The questions for the interview are prepared ahead of time as a guide around the research objectives. The respondents are probed to expatiate their response further when and where needed. The interview time varied between 30 minutes to one hour, depending on the respondent. Due to the aim of this research, the sample has been limited to participants with background information on expert knowledge who have experience and in IT security roles for at least five years and have at least two years' experience working in a Cloud environment. The semi-structured interview is chosen for this study because it provides an in-depth understanding of the context from respondents and usually makes use of open-ended questions (Jamshed, 2014).

An important consideration in qualitative research is in determining the sample size. The determination of the qualitative sample size is a very challenging one based

on different study designs and contextual considerations (Turner-Bowker et al., 2018, p. 842). Contrary to the quantitative research approach where the sample size can be calculated using statistical techniques, the qualitative sample size is calculated by the number of participants that are needed to attain saturation (Glaser, Strauss, & Strutzel, 1968, p. 61). The concept of saturation emerged when no more data are being found. A purposeful sampling size method is used as it suits the purpose of this study.

3.11.1.2 Survey

Surveys are a fixed set of questions for gathering information. They can be administered using paper or web form (Harrell & Bradley, 2009, p. 6). Similarly, Guyette (1983) described the survey as a method of collecting data consistently. A survey is a systematic way of gathering information from a sample of the population for establishing a meaningful variation (Guyette, 1983, p. 48). In quantitative studies, surveys are used for providing numerical distributions of variables, which is the statistical representation of the sample. In contrast, qualitative surveys are concerned with the diversity of a given population (Jansen, 2010, p. 4). Surveys are useful when the researcher intends to gain information about general patterns from a large population (Driscoll, 2011, p. 163). Qualitative surveys can be inductive or deductive. The inductive survey is often called open surveys, and they use open-ended questions which exclude pre-coded responses for the respondent. Deductive surveys make use of close-ended questions and are more structured than inductive designs.

Furthermore, surveys are also according to the instrument or time used (Sincero, 2016) According to instrumentation, surveys can be classified into questionnaires or interviews. A questionnaire is a paper and pencil instrument that is administered to respondents to gather information. The questions are usually designed as close-ended. Questionnaires have evolved over the past years in how they are administered. It includes self-administered, group-administered, and household drop-off (Sincero, 2016).

Surveys can be classified into longitudinal and cross-Sectional surveys based on the duration of time (Guyette, 1983; Visser, Krosnick, & Lavrakas, 2000; Sincero, 2016). Cross-Sectional surveys involve collecting information from respondents at a particular point in time concerning a particular behaviour, event, or phenomenon. One

of the critics of using a cross-Sectional survey is in the generalisation of findings. This is because the events, behaviour, or phenomena is that they are not constant. However, longitudinal surveys are used to gather information from a time to another to find the changes in the information gathered. There are three types of longitudinal surveys: panel, trend, and cohort (Avedian, 2014). The panel survey involves gathering information from the same participants over a period of time. In a trend survey, the researcher gathers information over a period of time from different participants in the same sample population. While in a cohort survey, the researcher is interested in gathering information over a period of time from a sample population with specific characteristics. The sample in a cohort survey may vary. While longitudinal surveys may gather rich data, they are costly and highly time-consuming. Also, there is a tendency for interrupted follow-up of participants (Caruana, Roman, Hernández-Sánchez, & Solli, 2015, p. 538).

In this study, a web-based survey is used for the pilot to gather preliminary information on the clarity of questions asked and the population. The survey questions are designed to gather information from IT security experts working in a Cloud environment. The questions consisted of open-ended and closed-ended questions. The closed-ended questions are to provide information on the demographics, while the open-ended questions are based on the research questions. Also, an anonymous survey is employed to recruit interview participants.

3.11.1.3 Documents analysis

Another method that is used in this study is through background documents in the area of study. It includes reviewing existing data in the form of databases, reports, or any other records. Bowen (2009, p. 28) described it as the systematic analysis of electronic or printed documents. These documents could include attendance registers, minutes of meetings, manuals, background papers, books and brochures, diaries and journals, organisational or institutional reports, survey data, and various public records (Bowen, 2009, p. 29). The document analysis method is particularly applicable to a qualitative approach and is usually used in combination with other qualitative methods. Documents provide useful rich background information and historical insight, especially for case study research. Furthermore, documents also provide insights into

questions that need to be asked during the study and a means to track any form of change and development (Bowen, 2009, p. 30). The method is most appropriate for this study because it is readily available through the university's e-library, and is cost-effective and efficient. For this study, the academic curriculum and professional certificates curriculum are utilised.

3.11.2 Data processing

Data processing involves checking the collected data and producing a meaningful output from the data. The checking activity includes checking for quality, completeness, and anonymity, and converting the collected data into a suitable format for conservation and dissemination (Guide, 2002, p. 2). The converting process involves adding contextual information to the data. Such as adding labels to interview tapes. The primary aim of the output generated during processing is to enable users to identify specific items in a data collection most relevant to their research (Guide, 2002). In this study, the collected data are from interviews and field notes. The interview tapes are ordered, organised, and labelled according to the questions or topics of discussion.

A series of actions or steps are performed on the data to verify, organise, transform, integrate, and extract data in an appropriate output form for subsequent use. Methods of processing must be rigorously documented to ensure the utility and integrity of the data. The primary aim of the stage is to prepare the data for analysis.

3.11.3 Data Analysis

Qualitative data analysis is the range of processes and procedures of transforming data that have been collected into some form of explanation, understanding, or interpretation of the people and situations being investigated (Taylor & Gibbs, 2010). The primary aim of data analysis in this study is to interpret the unstructured primary qualitative data that has been collected through interviews and an online survey. Generally, qualitative data analysis usually begins once there is data, and the steps involve getting familiar with the data, revisiting research objectives, developing a framework, identifying patterns and connections (Bhatia, 2018).

Several methods have been adopted in analysing qualitative data. Some of the widely used analyses are constant comparative analysis, narrative, thematic analysis,

discourse, ethnography, phenomenology, and grounded theory (Thorne, 2000; Dawson, 2009; Bhatia, 2018; Harding, 2018). Thematic analysis is a process of systematically identifying and organising and reporting themes within the data (Braun & Clarke, 2006, p. 6). It is particularly useful because of its flexibility for analysis. It is independent of theory or epistemology during analysis. Bruan and Clark (2006) identified six phases for doing thematic analysis: familiarization with the data, initial code generation, identifying themes, reviewing themes, defining and naming themes, and presenting the result (Braun & Clarke, 2006, p. 16).

For a case study, Yin (2003) advised that important strategies for analysing a case study are relying on theoretical propositions, thinking about rival explanations, and developing a case description (Yin, 2003, pp. 111-115). This suggests that the existing theory is the starting point of a case study. He described a case analysis as a form of pattern matching with the aim of explaining a case. He further suggests that to reduce personal bias; it is essential to test and identify any rivalry explanation as a result of a pre-conceived idea from the researcher. Also, to these strategies, he identifies some other techniques that can be used for case study analysis: pattern matching, explanation building, time-series analysis, logic models, and cross-case analysis. Similarly, Rowel (2002) suggests the best way to analyse a case study is to use prepositions that align with the research objectives (Rowley, 2002, p. 24). While Perry (1998), in a study, established that qualitative data analysis should be guided by a theory. In a case study, “data analysis consists of examining, categorising, tabulating, testing, or otherwise recombining evidence to draw empirically-based conclusions” (Yin, 2009, p. 126).

Following the data analysis processes outlined by Yin (2009) and the thematic analysis process, the underlying theoretical assumption for this study is to investigate the impact of Cloud computing on IT security skills and roles through a social construct with the underlying fact that knowledge is gain interactively. The data analysis steps can be seen in Table 3.6. The first step of analysis is the familiarization of the data, which involves annotating the transcribed data for preliminary observations. All primary data sources (the transcribed interview data and survey data) are imported into NVIVO data analysis software. The use of the software is to increase the efficiency and effectiveness of interpreting data and not replace the process of learning and

understanding from the data. It also provides rigour during analysis (Bazeley & Jackson, 2013, p. 2). Here, the transcribed data and survey data are read multiple times. Also, the interview tapes are listened to several times to identify recurrent themes. NVIVO has so many tools to help the researcher familiarize themselves with the data, such as word frequency and query search (Adu, 2016). Secondly, the categorization of data takes place. It involves the identification of themes in the data (Patton & Cochran, 2002). These themes may be a single word, sentence, or phrase. These themes are groups or categories created by comparing and contrasting the data. The process of identifying themes and patterns is referred to as coding. NVIVO uses nodes to save these themes. The nodes can be further categorized into parent nodes based on similar patterns and themes. These nodes are labelled and annotated with the researchers' description (Adu, 2016).

Table 3.6: Data Analysis Process

(Yin, 2009)

Yin's process for case study analysis	Description
Examining	<ul style="list-style-type: none"> • Bring in transcribed interview data and survey data. • Assigning labels and codes
Categorising	<ul style="list-style-type: none"> • Identifying patterns and relationships • Comparing relationships
Tabulating	<ul style="list-style-type: none"> • Use graphs, word trees, word frequency, and Tables Table to visualize data • Check for frequency and pattern of events
Testing or combining evidence to address initial propositions	<ul style="list-style-type: none"> • Comparison with existing literature • Description and implication of findings

Adu (2006) advised that the parent nodes should be used to address the research questions. Then a coding scheme is developed and finally applied to the whole data set. The third stage is tabulating; this stage involves presenting and visualising findings.

This could be in the form of word trees, word frequency, charts, tables, or maps. The explore tool in NVIVO is very helpful in this stage to visualize findings. With the explore tool, maps, tables, charts, and cluster trees can be created (Adu, 2016). The final stage is the testing phase, where a theory is tested or developed. This stage requires deeper understanding, synthesis, and possibly revisiting the data with new perspectives to make meanings and fully interpret the data (Bonello & Meehan, 2019). In this stage, a framework is constructed to disseminate the essence of the data for meaning. The testing stage is very important because that is where the result is presented. This stage largely determines the credibility of the study. The output of the data is expected to answer the research question by providing the skills needed by IT security professionals in the Cloud from a user organisation perspective. A summary of the research methodology used in this study is shown in Table 3.7.

Table 3.7: Summary of Research Methodology

Research Question	What are the impacts of Cloud computing on IT security roles?
Research Paradigm	Constructivism
Research method	Case study method
Data collection	Survey, Interview data, field notes, and documents
Data Analysis	Thematic and Triangulation analysis

3.12 SPECIFIC DATA COLLECTION STEPS

One of the advantages of using the case study method is that it allows for multiple data collection methods and techniques. Both primary data and secondary data are collected for this study. The primary data is collected using semi-structured interviews and surveys while the secondary data is collected from six university websites and five professional certification associations websites. The following section describes the steps for each of the data types.

3.12.1 Primary Data Collection Steps

The survey is done using an online survey tool, survey monkey. Survey monkey is easy to use and it provides a platform that allows easy tracking and measurement of

response. Survey monkey is set up using three types of questions, closed-ended, open-ended, and Likert questions. The closed-ended question is used to collect demographic information including years of experience in the profession, years of experience with Cloud, and the type of Cloud been used. The demographic questions are specifically designed not to ask any personal identifiable questions for the anonymity of participants. The Likert questions are used to measure the opinion of participants on the impact of Cloud computing on the required IT security skills and changing roles. The last part of the survey is designed with open-ended questions. The details of the survey questions are in Appendix B. An email containing the weblink is sent out to proposed respondents to collect survey responses. The purposive snowballing sampling method is used in collecting the survey response. The AUTECH Ethics approval is in Appendix A. Figure 3.2 summarizes the primary data collection steps.

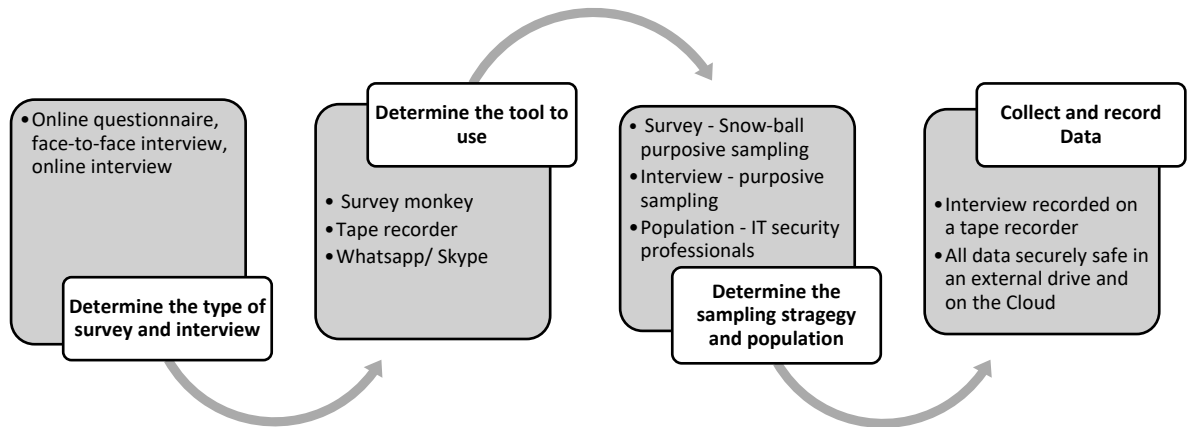


Figure 3.2: Specific Primary Data Collection Steps

The interview participants are from the survey respondents who met the criteria and shows interest in further study. The researcher asks the respondents to indicate their interest in a further survey for further studies through an interview. An email was sent out to all prospective participants along with the participant's information sheet and the informed consent asking them to choose a suitable time and location. The participant information provides a detailed process of the interview. A follow-up email is sent out a month later to those who are yet to respond.

The interview is conducted according to the participant's scheduled time. All the consent forms are received before the interview began. The interview began with thanking the participants for their time and contribution to the research. The participants are reminded the interview is voluntary participation and the informed consent is reconfirmed. During the interview, probes and follow-up questions are used to clarify the context of participants' responses. Also, questions are reiterated with examples when participants are unclear about the context, and participants are allowed to ask questions and give remarks. All the interview sessions are recorded using a tape recorder.

3.12.2 Secondary Data Collection Steps

The secondary data is collected using a curriculum from six New Zealand universities and five professional certifications curriculum. The six universities are selected based on QS ranking and the professional certifications are selected based on their curriculum and demand from employers. The documents are collected through university websites and professional security websites. The goal is to search for Cloud and security-related degrees or courses as the case may be. This is done using keywords and going through Computer Science, Information System, Cybersecurity, Information Security, Cloud computing, Computer Engineering, and Software Engineering. These keywords searched faster for any related program of interest. Each of the programs is then reviewed to identify any Cloud or security course for the six universities.

The professional certificates reviewed included both vendor-based and vendor-neutral certificates. The data is collected by listing the certificated and training offered by each of the professional bodies. The highly ranked security and Cloud courses are then reviewed. The goal is to review the domain expertise that is tested for each of the certifications. The data is carefully selected to capture the changes in skills requirements.

3.13 SPECIFIC DATA ANALYSIS TECHNIQUES

This Section discusses the specific techniques used to analyse the primary and secondary data collected for this study. The primary data is analysed using qualitative software, NVIVO, and the secondary data is analysed manually.

3.13.1 Primary Data Analysis Techniques

The primary data are analysed using the thematic analysis technique through a data qualitative software, NVIVO. NVIVO is chosen because it is a familiar software to the researcher and also provided by the institution. NVIVO 12.0 is used for this study. This Section describes the setup and use of NVIVO. The key components of an NVIVO project are sources, nodes, coding, and queries. Figure 3.3 describes the relationships between the components (Edhlund & McDougall, 2019, p. 12). Sources refer to the actual form of data that needs to be analysed. Nodes are flexible containers for data. It can be a part of the data or concepts or keywords used to describe an aspect of the data (Edhlund & McDougall, 2019, p. 12). Coding refers to the process of organising and categorizing data into nodes. Queries are a form of searches that provides ways of exploring data. Table 3.8 gives an overview of the components used in this study. Edhlund and McDougall (2019) described phases of how NVIVO can help organise data for easy analysis and conclusions. These are descriptive, thematic, and analytic coding. Figure 3.4 describes how it is applied in this study.

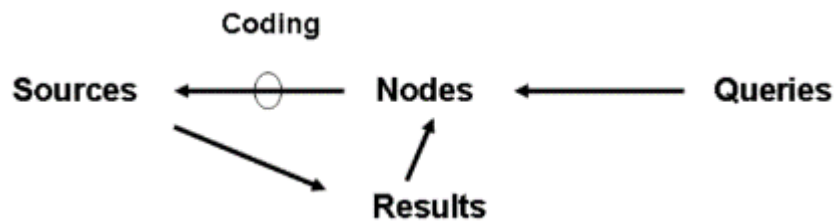


Figure 3.3: Components of NVIVO Project

(Edhlund & McDougall, 2019, p. 12)

The descriptive phase involves data familiarization which helps prepare the data for coding and analysis. The process involves creating, importing, and organising the data sources for the project into NVIVO as seen in Figure 3.5. The sources of data imported to NVIVO are survey data and interview transcripts. The survey data is imported directly from survey monkey. Survey monkey supports exporting data directly to NVIVO. The survey is in two parts and each part is imported separately. A folder is

created separately for the participants and respondents. Both the interview participants and survey respondents are coded using P01 – P20 for anonymity.

Table 3.8: The Components of NVIVO Project for The Study Adapted

Components	Description
Sources	Survey data, interview transcript
Nodes	90 initial nodes are created
Coding	Descriptive, thematic, and analytic
Queries	Cross case queries

The second stage is the thematic stage. It involves exploring the data to create initial coding. This stage is where the coding process begins. At this stage, 90 nodes are created from the data. Each node contains a selection of text from the participant and respondents. These are phrases that are used to group related concepts related to answering the research questions. Figure 3.6 shows the process of creating the nodes. The nodes are manually created by going through the data sources and identifying patterns.

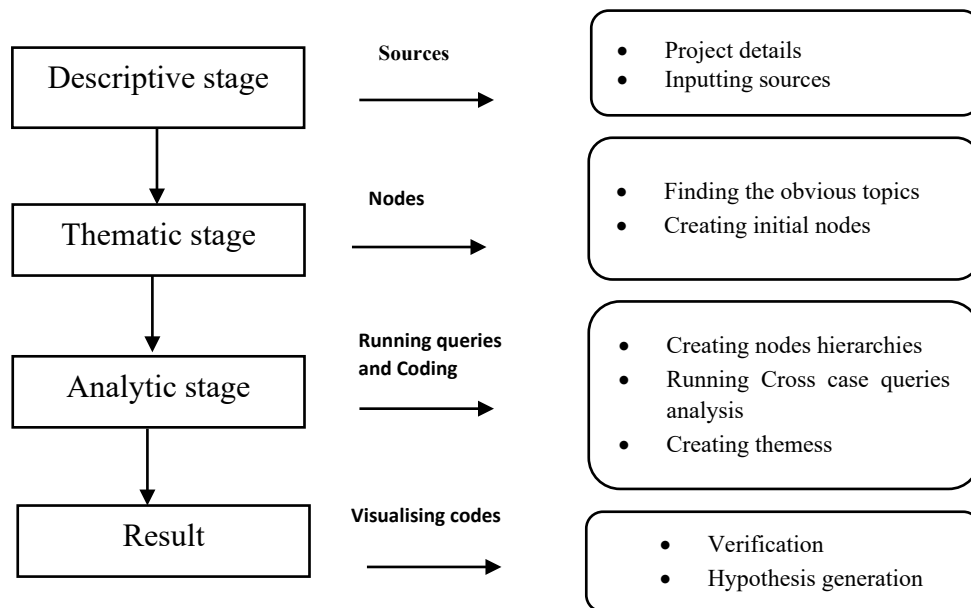


Figure 3.4: The Stages of Using the NVIVO Project

(Adapted from (Edhlund & McDougall, 2019))

The analytic stage involves merging the initial nodes into hierarchies to communicate analytic findings. In this stage, a total of seven themes are created from the initial 90 codes. This is the most time-consuming stage as it involves careful reviewing, analytic thinking, and categorizing of codes. It involves a continuous coding process of revisiting narratives and discussions, renaming, and creating new codes to enhance the analysis. Figure 3.7 shows the node hierarchy for the theme one classification.

The top screenshot displays the 'Interview Transcript' data source in NVivo 12 Pro. The interface includes a sidebar with 'Quick Access' (Files, Memos, Nodes) and 'Data' (Files, Demographic, Interview Transcript, Survey). The main pane shows a table with columns: Name, Codes, References, and Modified On.

Name	Codes	References	Modified On
P01	4	8	7/13/2020 12:18 PM
P12	40	59	7/13/2020 12:16 PM
P14	85	243	7/13/2020 12:16 PM
P15	71	123	7/13/2020 12:15 PM
P17	87	162	7/13/2020 12:17 PM
P18	39	50	7/13/2020 12:16 PM
P19	59	111	7/13/2020 12:17 PM

The bottom screenshot displays the 'Survey' data source in NVivo 12 Pro. The interface is similar to the top one, but the main pane shows a table with columns: Name, Codes, References, and Modified On.

Name	Codes	References	Modified On
First questionnaire	138	764	7/14/2020 3:04 PM
second questionnaire	160	925	7/14/2020 3:04 PM

Figure 3.5: NVIVIO Data Sources

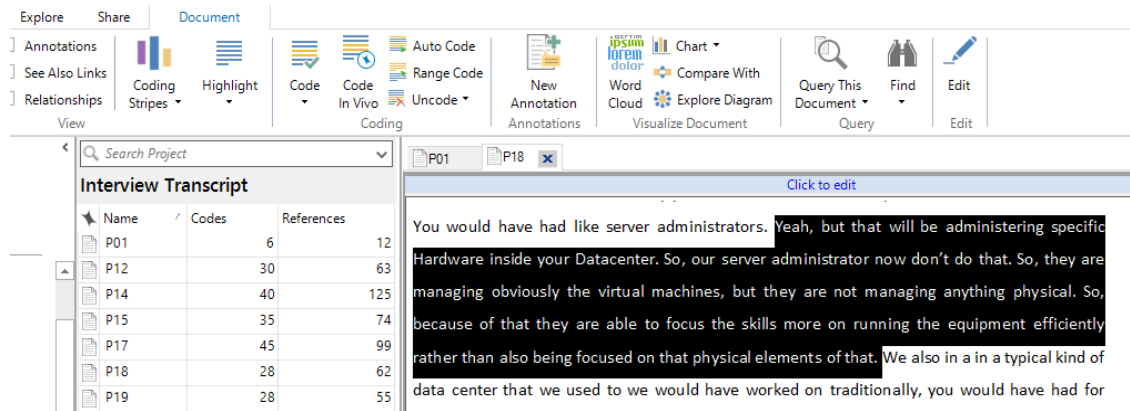


Figure 3.6: Creating Nodes in NVIVO

For example, in theme one, skills are categorized into technical and non-technical skills. There is a clear pattern in the list of important skills from the initial coding. The technical skills are further classified into security and basic skills. Furthermore, the explore tool in NVIVO is very helpful in this stage to visualize findings. This study uses the chart, mind maps, query wizard. The findings are described in Chapter four.

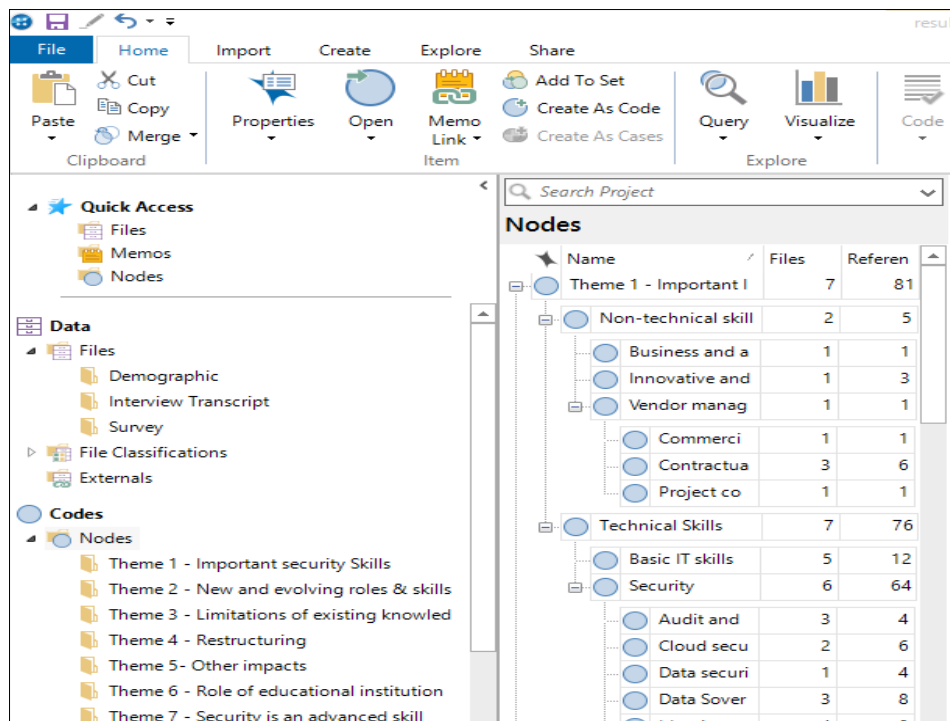


Figure 3.7: Nodes Hierarchy Organisationin NVIVO

3.13.2 Secondary Data Analysis Techniques

The secondary data are analysed manually. It comprised data from university-specific professional certification websites. It is easier to manually analyse these data that are extracted directly from websites and the volume of information is manageable. The information is recorded for each school and certification. Specifically, security-related programs and programs that teach security courses are reviewed from individual university websites. Finally, the data are compared and tabulated.

3.14 LIMITATIONS

The research method chosen for this study is expected to provide a reliable way of collecting and analysing data and provide an answer to the research questions. However, like any other research methodology, the chosen research methodology has its limitations. Qualitative research has been criticized for its lack of scientific rigour and lack of transparency in its analytical procedures and findings because it is subject to the researcher's bias (Rolfe, 2006). This Section discusses the limitations and their impact on research. Reliability and validity are two major aspects of research that can assert rigour and are necessary to measure quality (Cypress, 2017, p. 254).

3.14.1 Reliability

Reliability is the measure of the accuracy of the proposed research method. It measures how accurate the method can meet the proposed research question. Leung (2015) referred to reliability as the replicability of the research process and results. Reliability can also be described as the consistency of analytic procedures and details of how personal and research method bias could influence findings (Noble & Smith, 2015, p. 3).

The issue of reliability in qualitative research is a very complex one because of the challenges involved in replicating the exact conditions under which a piece of evidence or data was originally collected. Carcary (2009) reports that even if the same participates in a later similar study, it is unlikely they would provide identical responses (Carcary, 2009, p. 14). For example, one research tool used in this study is the interview. Hence, the participant's response is somewhat dependent on the questions asked, and their understanding of the current issue. This is subject to change over time.

This is why the issue of reliability in qualitative research is focused on consistency. A margin of variability is tolerated in qualitative research, provided the methodology and epistemological views produce ontologically similar data but may differ in richness and ambience within similar studies (Leung, 2015). This study ensures the data collection, analysis, and interpretation of findings is clear and transparent by detailing every process that led to the findings. Also, triangulation and checking are used to enhance reliability.

3.14.2 Validity

Validity is ensuring the trustworthiness of the findings is maximized (Patton & Cochran, 2002, p. 26). It is the appropriateness of tools, processes, and data during a research process. Validity is assessing whether the research question, chosen methodology, research design, and sampling size and analysis method are appropriate or accurate for the desired outcome (Leung, 2015). Babour (2001) identified the checklists that can improve the qualitative research method. He reveals that these checklists could strengthen the rigour of qualitative research only if embedded into the process of qualitative research design and data analysis. Similarly, Yin (2009) outlines three types of validity: construct, internal, and external. Construct validity can be achieved through the triangulation of multiple sources of evidence, chains of evidence, and member checking. Internal validity can be established through the use of established analytic techniques such as pattern matching, while external validity is achieved through analytic generalisation. Table 3.9 describes the criteria used in achieving reliability and validity in this study.

Table 3.9: Criteria for trustworthiness of data

Quality elements	Criteria	Description of Strategy
Reliability or Consistency	Transferability	<ul style="list-style-type: none">• Thick Description: Provided rich details of participants, procedure, and context of the present study• Maintained files or records of raw data from both survey and semi-structured interviews, audio files of all interviews, interview narratives and transcripts, field notes, researcher's memo.
Validity or Trustworthiness	Credibility	<ul style="list-style-type: none">• Method Triangulation: Multiple data collection triangulation through an online questionnaire, survey, and interviews• Persistent observation: Identifying those characteristics and elements that are most relevant to the problem or issue under study, on which you focus in detail.
	Dependability and Confirmability	<ul style="list-style-type: none">• Audit trails: In-depth research processes are clearly provided, and details are documented.• Admitting research beliefs, assumptions, and shortcomings• Ensuring uniformity of questions that the participants are asked

		<ul style="list-style-type: none"> • Used qualitative data analysis software (NVIVO) in data reduction, reconstruction, synthesis products, and reflexive journals
--	--	---

Furthermore, Lincoln and Guba (1985) suggest that the trustworthiness of research can be achieved through transferability, credibility, confirmability, audit trails, and dependability criteria (Lincoln & Guba, 1985, p. 290). *Credibility* addresses the issue of internal validity by ensuring the original representation of the respondent's view is presented by the researcher. It measures the level of confidence that can be placed in research findings (Korstjens & Moser, 2018, p. 121). It can be achieved using engagement, persistent observation, triangulation, peer debriefing, member checks, saturation, prolonged contact, reflexivity, and external checks on the research process (Lincoln & Guba, 1985; Simon & Goes, 2016). *Transferability* relates to external validity. It explains the degree to which the findings of a study can be applied to a similar context or settings from the actual study (Korstjens & Moser, 2018; Chutikulrungssee, 2020). Transferability can be strengthened through a thick description that sufficiently describes the research process in detail. Transferability is a major challenge in qualitative research. This is due to the inherent subjectivity of qualitative research and the potential for the researcher's bias. It is, therefore, essential to conducting research with extreme rigour (Cypress, 2017, p. 254). *Dependability* measures the consistency of findings over time. It addresses issues of reliability of a study, whether the same result can be obtained when the study is repeated in the same context, using the same participants and methods (Shenton, 2004). Dependability can be achieved through triangulation – using multiple overlapping methods. *Confirmability* is the degree to which others can confirm the findings of a study. It entails ensuring the findings is the actual interpretation of the participant's view and not the researchers (Korstjens & Moser, 2018). Confirmability is closely related to dependability, it can be demonstrated where dependability is established (Lincoln & Guba, 1985, p. 316). It can be achieved through audit trails and triangulation.

3.15 CONCLUSION

In conclusion, this Chapter provided the methods, methodology and theoretical assumptions used for this study. It presents a review of similar studies and their methods. The issues and challenges identified from Chapter two are reviewed and analysed. This helped to focus on the research problem area. One researchable problem has been selected, and three hypotheses developed to guide the research. The qualitative methodology is adopted for this study. Furthermore, the widely used theoretical assumptions and methods used in qualitative studies are described, and the constructivist approach is adopted for this study.

The case study method is extensively described, and the semi-structured interviews and surveys are the instruments chosen for collecting data. Also, the comprehensive process by which the data is analysed and presented is set out. Finally, it discusses the possible limitations of this methodology that have been presented and ways of mitigating the potential risks of these limitations. Chapter four reports the findings based on the chosen methodology defined in this Chapter.

Chapter Four

Results

4.0 INTRODUCTION

It is necessary to make meaning from the data to realize the aim of the research and answer the research questions. The primary sources of data are interviews and surveys. The secondary sources are course curriculum and professional certification data from websites. Chapter three shows that the data is interpreted using thematic analysis, and data analysis is done using NVIVO 12.0 software.

Chapter four presents the findings of the data collected from the qualitative descriptive multiple case study. The results are presented using Yin's (2009) stages of case study analysis. Overall, six main themes emerged, and each of these themes is explained using Tables, graphs, and excerpts from the data.

4.1 DEMOGRAPHICS

This section describes the sample of the population that is used in data collection. An online survey, interview, and documents are used to collect empirical data for this study. The participants are industry experts and selected based on their expert knowledge and experience working in an IT security traditional environment as well as working in the Cloud environment. The research population is IT security Professionals in NZ. Section 4.1.1 describes the survey demographics, Section 4.1.2 describes the interview demographics, and Section 4.1.3 outlines the sample of the document collection.

4.1.1 Survey Demographics

There are two rounds of surveys used for data collection. The first survey is designed to understand the important skills and how efficient traditional skills are when working with the Cloud. The link to the online survey is emailed to respondents (see Appendix B). The questions are open-ended, providing respondents with a deep and lengthy response.

The second survey is modified based on then the feedback from trusted professionals and peer review to clarify some of the language used in the questions. Also, some questions have sub-question to get a clearer response from respondents. The second survey is divided into three parts: a demographic section, Likert questions, and open-ended questions. Open-ended survey questions made it possible to gather deep insight into real-life situations from participants based on their knowledge and experience. The questions are focused on the overall impact of skills on the changes the Cloud brings to IT security professionals. After a limited response for nearly two months, follow-up emails are used to give a reminder. They are also asked to invite professional colleagues to participate in using snowball sampling. A total of 20 responses completed the second online survey. Both surveys are designed using the survey monkey online tool. For interview purposes, the participants who are interested in a further interview study provided their email addresses and are contacted. Table 4.1 and 4.2 give an overview of the participant's professional details.

Table 4.1: First Survey Demographics

Group	Number	Percentage (%)
Job function		
Auditors	4	44.44
Risk Analyst	1	11.11
IT manager	1	11.11
Teacher/Prof	1	11.11
Support Admin	2	22.22
Industry		
Academia	4	44.44
IT consulting	5	55.56

Table 4.2: Second Survey Respondent's Demographic

Respondent	Job title	Years of experience	Years in current position	Cloud service or environment deployed by your organisation	Years using Cloud services?	Volunteered for interview
P01	Audit Manager, Technology	10+ years	0-3years	AWS and Azure (PaaS, IaaS, SaaS)	0-3years	Yes
P02	IT Audit Manager	3-6years	0-3years	IaaS, SaaS	5+ years	No
P03	Internal Auditor	7-10years	0-3years	SaaS	5+ years	No
P04	Audit Manager	0-3years	0-3years	Microsoft Azure	0-3years	Yes
P05	Network Engineer	10+ years	0-3years	AWS	0-3years	Yes
P06	Intermediate Developer	0-3years	0-3years	AWS	0-3years	Yes
P07	AWS Specialist	3-6years	0-3years	Public Cloud	0-3years	No
P08	Cloud Engineer	10+ years	0-3years	Private Cloud	0-3years	Yes
P09	Information Security Analyst	0-3years	0-3years	AWS / Azure	0-3years	No
P10	Audit Manager	3-6years	0-3years	Sharepoint	3-5years	No
P11	IT manager	10+ years	7-10years	IaaS, PaaS, SaaS	3-5years	No
P12	Senior Systems Administrator	7-10years	0-3years	IaaS SaaS	0-3years	Yes
P13	Cloud Security Advisor	3-6years	3-6years	Hybrid	3-5years	No
P14	Solution Specialist - Security Architecture	0-3years	0-3years	Both Microsoft Azure and Amazon Web Services	0-3years	Yes
P15	Chief Technology Officer	10+ years	0-3years	AWS Serverless	0-3years	Yes
P16	IT Consultant	3-6years	0-3years	Azure / AWS	0-3years	No
P17	Site Reliability Engineer	0-3years	0-3years	Openstack, Vcenter, Hyper-V Cloud	3-5years	Yes
P18	Senior security risk analyst	7-10years	0-3years	Xero, Software as a service	5+ years	No
P19	IT platform manager	7-10 years	0-3years	Azure / AWS	0-3years	Yes
P20	Lecturer	10+	0-3	Azure and AWS	0-3	No

4.1.2 Interview Demographics

The participants who volunteered in the second survey are contacted via email. Although there are initially ten volunteers for the interview, only six responded to follow-up emails and are scheduled for an interview (See Appendix D). The participants are asked common questions regarding the impact Cloud computing is having on IT security skills and are encouraged to elaborate on their opinions. They are all active users of Cloud technology. Table 4.3 outlines the demographic of interview participants.

Table 4.3: Interview Participant's Demographics

Group	Number
Job function	
Chief Technology officer	1
Senior Security Risk Analyst	1
Solution Specialist (Security Architecture)	1
IT platform Administrator	1
Senior System Admin	1
Site Reliability Engineer	1
Industry	
Cloud security	1
Technology	1
IT services	1
Telecommunications	1
Insurance	1
Power	1

4.1.3 Documents Demographics

The document is collected manually from seven Universities and six professional certification association websites. The seven Universities are selected based on QS ranking and undergraduate programs. The professional certifications included five vendor-neutral and one Cloud-specific certification. These are selected based on their curriculum and demand from employers.

Table 4.4: Sample of Reviewed Documents

Group	Programs	Courses
Universities		
University of Auckland	2	6
University of Otago	2	3
Auckland University of Technology	1	5
University of Canterbury	3	4
University of Waikato	2	4
Victoria University	3	10
Massey University	1	2
Professional body		
Cloud Security Alliance (CSA)	1	14
Information Systems Audit and Control Association (ISACA)	3	13
The International Information System Security Certification Consortium (ISC2)	3	21
CompTIA	2	10
CISCO	2	27

4.2 CODE ANALYSIS

The analysis is done using NVIVO 12.0 analysis software. The analysis follows Yin's (2009) stages of analysis – examining, categorizing, tabulating, and testing, and the thematic analysis framework. Each stage of analysis is explained in Section 4.2. Table 4.5 outlines how data trustworthiness is achieved for each stage of the analysis.

Table 4.5: Achieving Data Trustworthiness During Data Analysis

Yin's Process	Thematic Analysis stages	Trustworthiness criteria	Description
Examining	Familiarize yourself with your data.	Audit Trials	<ul style="list-style-type: none"> • Persistent observation. • Identifying those characteristics and elements that are most relevant to the problem or issue under study, on which you focus in detail. • Documentation of all surveys, field notes data and interview transcript. • Organising all data in archives.
Categorizing	Generate Initial code Assign preliminary codes to your data in order to describe the content.	Dependability	<ul style="list-style-type: none"> • Triangulation • Documentation of code generation through NVIVO.
	Search for patterns or themes in your codes across the different interviews.		
Tabulating	Review themes.	Credibility	<ul style="list-style-type: none"> • Triangulation
	Define and name themes.		
Testing or combining evidence to address initial propositions	Produce your report	Confirmability, Transferability	<ul style="list-style-type: none"> • Thick description of all the stages of the research process

4.2.1 Phase One – Examining

The first stage of the analysis is examining the data coding. All the interview transcripts, survey responses, and field notes are uploaded into the software, and a folder structure for the data repository is created. The next step is to get familiar with

the data. The process of achieving this included listening to recordings, reading interview transcripts, and field notes annotating the transcribed data for preliminary observations. Ideas and potential codes to use are documented. Figure 4.1 shows the folder structure in NVIVO.

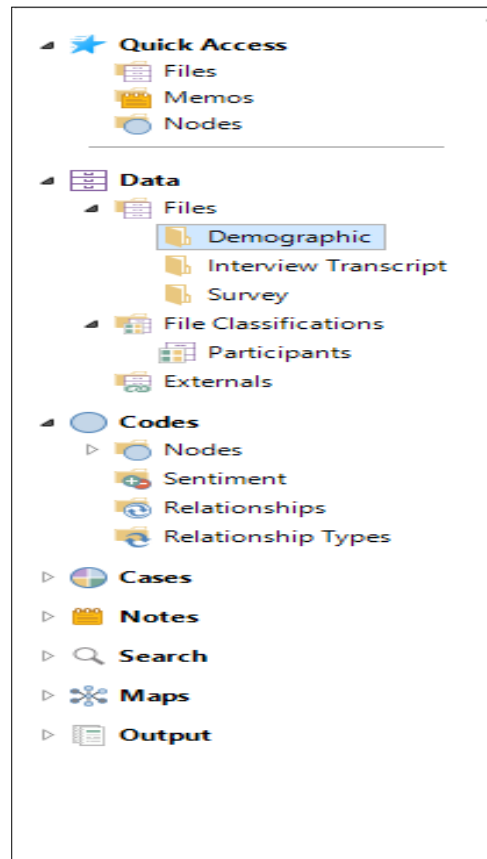


Figure 4.1: Folder Structure

4.2.2 PhaseTwo – Categorizing

This stage involved breaking down the organised data into phrases, sentences, or paragraphs to identify patterns and relationships in and across the data. NVIVO software helped in data reduction and de-construction, which is guided by the research questions. Given this, the data is coded to capture something relevant to the research questions. Each of these sentences or phrases is labelled and created into nodes in NVIVO. Figure 4.2 shows the initial codes that are created. A total of 90 initial codes are created.

Nodes							
Search Project							
Name	Files	References	Created On	Created By	Modified On	Modified By	
Have a general certificate and a vendor specific		4	5/3/2020 11:53 AM	AA	13/07/2020 11:39 AM	AA	
Basic IT skills		1	2/26/2020 6:13 AM	AA	26/06/2020 7:02 AM	AA	
Need to review the fundamental technical concepts		6	7/2/06/2020 6:57 PM	AA	9/06/2020 11:17 AM	AA	
Educational institutions not ready for the change		1	1/23/05/2020 2:23 PM	AA	23/05/2020 3:09 PM	AA	
Security and cloud skills should be taught in informal settings by external bodies		3	4/23/05/2020 3:11 PM	AA	4/06/2020 1:49 PM	AA	
Application development		1	1/8/06/2020 6:53 AM	AA	8/06/2020 6:53 AM	AA	
Security is an advanced level qualification		3	6/24/05/2020 6:11 AM	AA	4/06/2020 2:16 PM	AA	
Security should not be a basic course in school		2	3/24/05/2020 6:12 AM	AA	4/06/2020 2:47 PM	AA	
Self-development is key in security		1	1/24/05/2020 6:26 AM	AA	24/05/2020 6:26 AM	AA	
cloud service certification is important		6	9/24/05/2020 6:59 AM	AA	26/06/2020 10:33 AM	AA	
Changing roles		3	5/23/05/2020 2:07 PM	AA	7/06/2020 6:54 AM	AA	
People with certifications are seen to be more qualified		1	2/3/06/2020 5:57 PM	AA	4/06/2020 6:15 AM	AA	
Educational system does not need to adjust		1	1/5/06/2020 6:43 AM	AA	5/06/2020 6:43 AM	AA	
Issue of proprietorship makes cloud skills difficult		1	2/5/06/2020 1:30 PM	AA	5/06/2020 1:56 PM	AA	
Formal education is important for security and University play a key role		1	1/5/06/2020 1:41 PM	AA	5/06/2020 1:43 PM	AA	
Universities can't teach what is not standardized		1	1/5/06/2020 1:57 PM	AA	5/06/2020 1:57 PM	AA	
Basic IT skills are helpful relating to working cloud services.		2	8/7/06/2020 6:18 AM	AA	9/06/2020 10:49 AM	AA	
IAAS		2	3/9/06/2020 5:54 AM	AA	9/06/2020 11:15 AM	AA	
Basic IT skills are not sufficient to work in cloud environments		2	11/7/06/2020 6:53 AM	AA	26/06/2020 5:55 AM	AA	
Security roles and skills does not change		1	2/7/06/2020 5:43 PM	AA	7/06/2020 5:47 PM	AA	
Basic technology concepts		2	5/4/06/2020 2:03 PM	AA	5/06/2020 11:08 PM	AA	
Security roles hasn't changed		1	1/9/06/2020 6:24 AM	AA	9/06/2020 6:24 AM	AA	
Staff reduction is dependent on the extent of cloud usage		1	1/9/06/2020 6:35 AM	AA	9/06/2020 6:36 AM	AA	
Cloud skills is still scarce		1	5/26/06/2020 10:57 AM	AA	26/06/2020 8:04 PM	AA	
Cloud skills can be easily picked up		1	2/26/06/2020 11:27 AM	AA	26/06/2020 11:27 AM	AA	
Enhanced security		3	3/23/05/2020 7:44 AM	AA	4/06/2020 9:25 AM	AA	
It provides the opportunity to enhance security but does not necessarily enhance		4	8/4/06/2020 6:28 AM	AA	5/06/2020 10:05 PM	AA	
Vendor-neutral provides the basic general skills		1	1/23/05/2020 3:14 PM	AA	23/05/2020 3:14 PM	AA	
Vendor-specific is for defined career path		4	4/23/05/2020 3:15 PM	AA	7/06/2020 5:40 PM	AA	
Network and Data Admin roles		2	6/7/06/2020 6:29 AM	AA	26/06/2020 4:39 PM	AA	
Physical or Hardware security jobs		2	4/26/06/2020 7:04 AM	AA	26/06/2020 4:39 PM	AA	
Security Architect		1	1/8/06/2020 6:21 AM	AA	8/06/2020 6:21 AM	AA	
Security Engineer		1	1/8/06/2020 6:22 AM	AA	8/06/2020 6:22 AM	AA	
Security Infrastructure Engineer		1	3/8/06/2020 6:23 AM	AA	8/06/2020 6:53 AM	AA	

Figure 4.2: Initial Coding in NVIVO

Then, each of these codes is systematically reviewed, modified, and categorized into broader groups (themes). At the end of this process, codes have been organised into broader themes with extended meanings. The review resulted in merging, renaming, or clustering of nodes into related categories. The emerging ideas are reconstructed into a broader hierarchical theme known as tree nodes in NVIVO. For example, grouping skills together as essential skills required to work with Cloud computing technology. A total of eight themes emerged, and the themes are predominantly descriptive. Figure 4.3 gives an example of node categorization in NVIVO.

Nodes Search Project		
Name	Files	References
Theme 1 - Important IT security skills	0	0
Non-technical skills	0	0
Business and analytical	1	1
Commercial management and cost optimizatio	1	1
Innovative and critical thinking	1	3
Technical Skills	0	0
Basic IT skills	1	2
Cloud security	2	7
Coding	4	8
Compliance monitoring and reporting	1	2
Cyber security skills	1	1
Data security and privacy issues	1	4
Data Sovereignty	1	5
Governance and contractual controls	4	9
Identity and Access management	4	8
Infrastructure management	1	1
Major cloud provider skills	1	1
Network and Infrastrure Security	3	3
Project management skills	1	1
Risk Assessment and Management	3	21
Scripting	2	2
Security assurance and audit control	2	2
Service management	1	1
Traffic management	1	1
Virtualization security	1	1
Theme 2 - New and evolving roles & skills	0	0
Changing job roles	0	0
Application development	1	1
IT Support or Helpdesk roles	0	0
Network and Data Admin roles	2	6
Physical or Hardware security jobs	2	5
Security Architect	1	1

Figure 4.3: Categorizing of Nodes into Broader Themes

4.2.3 Phase Three – Tabulating

This phase involves presenting the result through Tables, charts, maps, and Figures of the findings. The explore function in NVIVO is used to create project maps, concept maps, charts, and cluster trees. These visualization tools show relationships between nodes across participants. The results are presented according to the identified themes.

4.2.3.1 Descriptive analysis

This Section provides a descriptive analysis of the closed-ended questions of the survey. It provides a statistical summary of the collected data. The analysis is divided into the following two parts to describe each of the surveys.

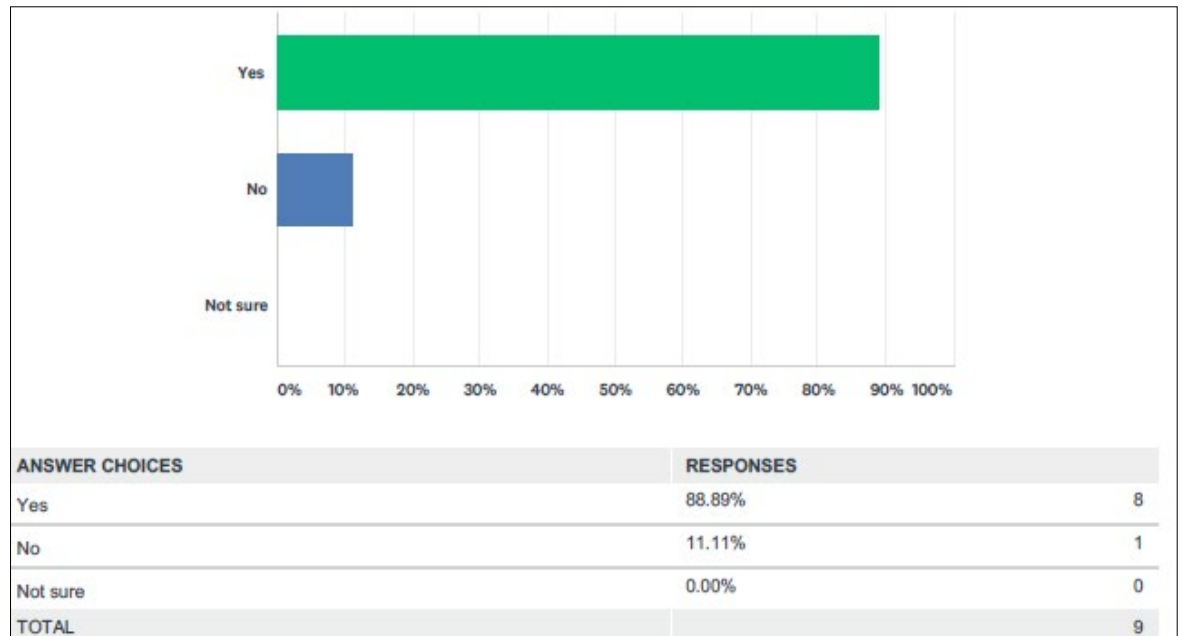


Figure 4.4: Respondents' view on whether new skills are needed to cope in the Cloud environment?

The first survey contained five array close-ended questions with a short description (see Appendix B). The summary of these questions can be seen in Figure 4.4, 4.5, 4.6, 4.7, and 4.8, respectively. All the respondents agreed that there's going to be a significant change in the IT staffing model and that Cloud computing affects the staffing model. The overall staffing and organisational strategy have shifted.

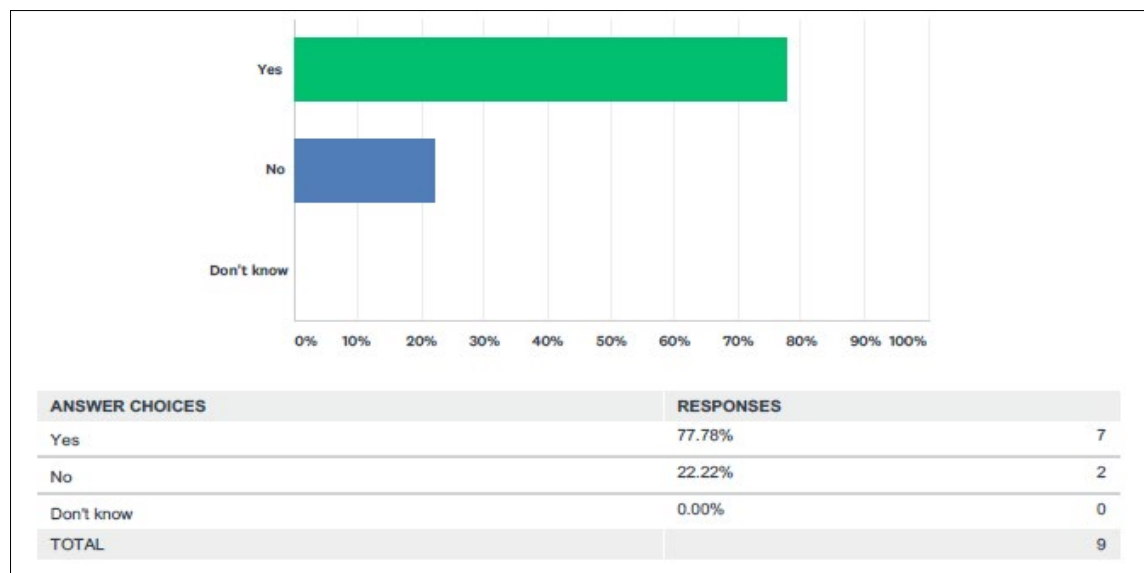


Figure 4.5: Respondents' View on Whether the Type of Cloud or Cloud Service Determines the Required IT Security Skills

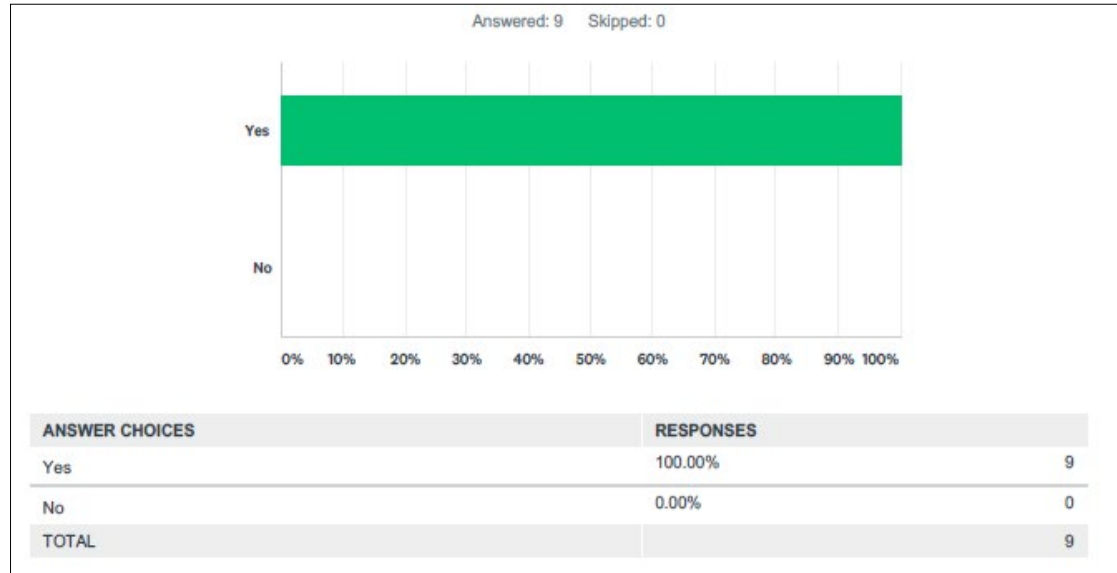


Figure 4.6: Respondents' View on Whether the Cloud is Causing A Significant Change in IT Staffing Model

Eight of the experts believe new skills are needed to cope in the Cloud environment. These skills they believe are dependent on the organisation, the Cloud service, the roles and responsibility of the employee, and the cost. While most of the participants believe there is a need for upskilling to cope in a Cloud environment, the required skills are based on the size of the organisation, financial capability, goal and strategy, type of Cloud, and Cloud service.

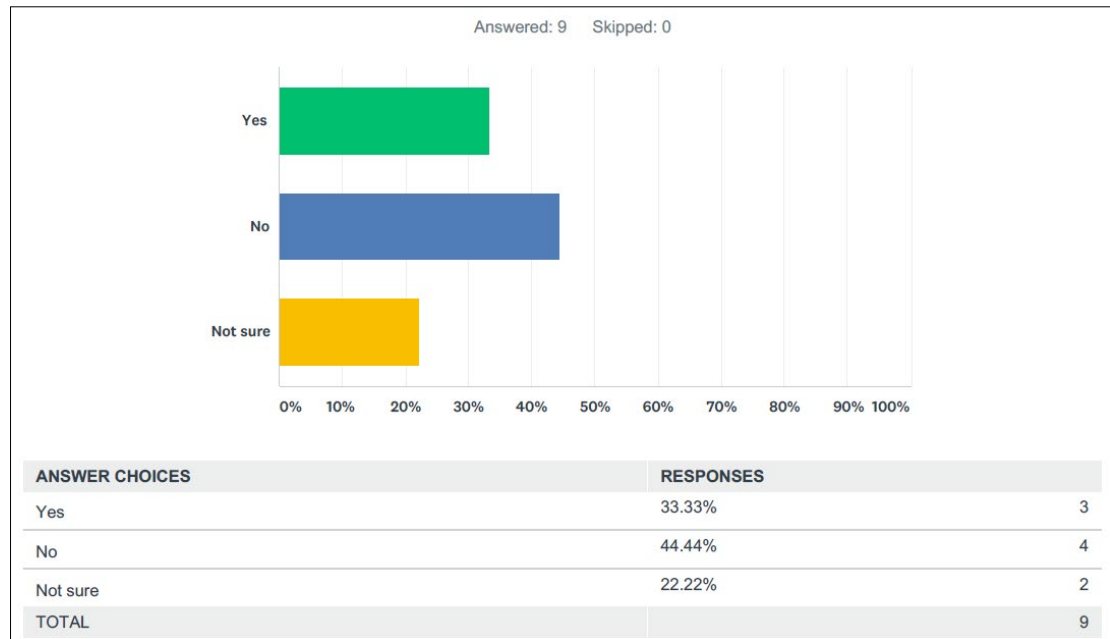


Figure 4.7: Respondents' View on Whether Some Skills and Jobs Become Irrelevant in the Cloud

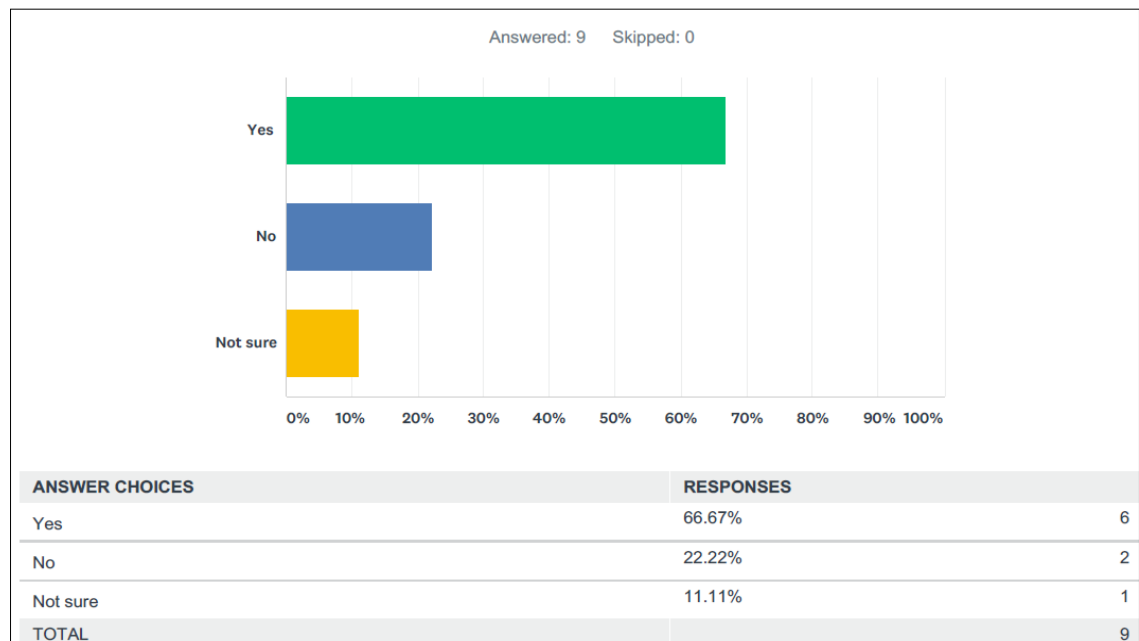


Figure 4.8: Experts' View on Traditional Skills Efficiency in Cloud Computing

The second online survey contained nine Likert questions to understand the perception of the respondents on the changing skills and roles. Likert questions are useful in understanding opinions, measuring attitudes, or an individual's reflection of reality (Göb, McCollin, & Ramalhoto, 2007, p. 604). One of the popular ways of analysing Likert questions is through an implicit interpretation of the Likert scale using a weighted average. The scores are calculated based on the arithmetic averages of the respondent scores. Table 4.6 shows the Likert scores of respondents' answers for each question. The numbers on each scale represent the number of respondents' responses to the questions, while the percentage score is the corresponding percentage of respondents' responses. For example, in Table 4.6 on the first question, five respondents, which corresponds to 25% of the total, strongly disagree that the basic IT skills are sufficient to work with the Cloud.

Table 4.6: Descriptive Characteristics

Question	Strongly disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly agree	Total	Weighted average
The basic or traditional IT security knowledge and skills are sufficient when working with Cloud	25.00% 5	35.00% 7	15.00% 3	20.00% 4	5.00% 1	20	2.45
Cloud has changed the skill sets required by IT security professionals	5.00% 1	5.00% 1	5.00% 1	65.00% 13	20.00% 4	20	3.90
The type of Cloud deployed, or Cloud service determines the skills sets of IT security professionals	0.00% 0	0.00% 0	25.00% 5	70.00% 14	5.00% 1	20	3.80
Some IT skills will become	0.00% 0	5.00% 1	25.00% 5	55.00% 11	15.00% 3	20	3.80

irrelevant with the use of Cloud							
The needed skills for IT security professionals are the same with or without Cloud	25.00% 5	25.00% 5	15.00% 3	35.00% 7	0.00% 0	20	2.60
Using Cloud services in an organisation changes the job roles/responsibilities of IT security professionals	0.00% 0	10.00% 2	0.00% 0	70.00% 14	20.00% 4	20	4.00
The type of Cloud or Cloud service deployed determines the roles of IT security professionals	0.00% 0	15.00% 3	5.00% 1	70.00% 14	10.00% 2	20	3.75
Using Cloud services affect IT staffing in an organisation	0.00% 0	0.00% 0	15.00% 3	65.00% 13	20.00% 4	20	4.05
Some of the IT security job roles are becoming redundant	10.00% 2	20.00% 4	20.00% 4	40.00% 8	10.00% 2	20	3.20

4.2.4 Phase Four - Findings

After the categorizing stage, a total of six themes are created from the data. Table 4.7 outlines the themes category (sub-themes) and codes generated from NVIVO. Figure 4.9 outlines the summary of participants' responses to each of the themes.

Table 4.7: Theme Identification

Main Theme	Category	Codes
Important IT security skills	<ul style="list-style-type: none"> - Non-technical skills - Technical Skills 	<ul style="list-style-type: none"> • Business and analytical • Contractual controls • Innovative and critical thinking • Vendor management <ul style="list-style-type: none"> ○ Project coordination ○ Commercial and cost optimisation ○ Contractual controls • Basic IT skills • Security <ul style="list-style-type: none"> ○ Audit and governance ○ Cloud security ○ Data security and privacy issues ○ Data Sovereignty ○ Identity and Access management ○ Major Cloud provider skills ○ Network and Infrastructure Security ○ Risk Assessment and Management ○ Virtualisation security
New and evolving roles & skills	<ul style="list-style-type: none"> - Changing job roles 	<ul style="list-style-type: none"> • Application development • Network and Data Admin roles • Physical or Hardware security jobs • Security Infrastructure Engineer • System Admin roles

	<ul style="list-style-type: none"> - New roles 	<ul style="list-style-type: none"> • Cloud Architects • Cloud security engineer • Commercial management and cost optimisation • Configuration management • Risk analyst • Security Architect • Security Infrastructure Engineer (Cloud-CP)
Limitations of existing knowledge and skills	<ul style="list-style-type: none"> - A need for broader knowledge - Proprietary of various Cloud providers - Traditional skills are not so relevant 	<ul style="list-style-type: none"> • Cloud requires specific skills • Roles and responsibilities are changing
Other impacts	<ul style="list-style-type: none"> - Direct Skills and roles impact <ul style="list-style-type: none"> ○ Restructuring <ul style="list-style-type: none"> ▪ New skillset ▪ Firing and Hiring new - Indirect Skills and Roles impact <ul style="list-style-type: none"> ○ Cost management ○ Enhances security ○ Focus on business core 	<ul style="list-style-type: none"> • Emphasis on industry certifications and training • Job loss and reduced staffing • Hiring skilled staffs • Roles migration and adaptation
Role of the HEI	<ul style="list-style-type: none"> - Review the curriculum - Teaching relevant skills 	

Learning Security Skills	<ul style="list-style-type: none"> - Emphasis on certifications and training - Security and Cloud skills should be taught in informal settings by external bodies - Security is an advanced level qualification 	
---------------------------------	--	--

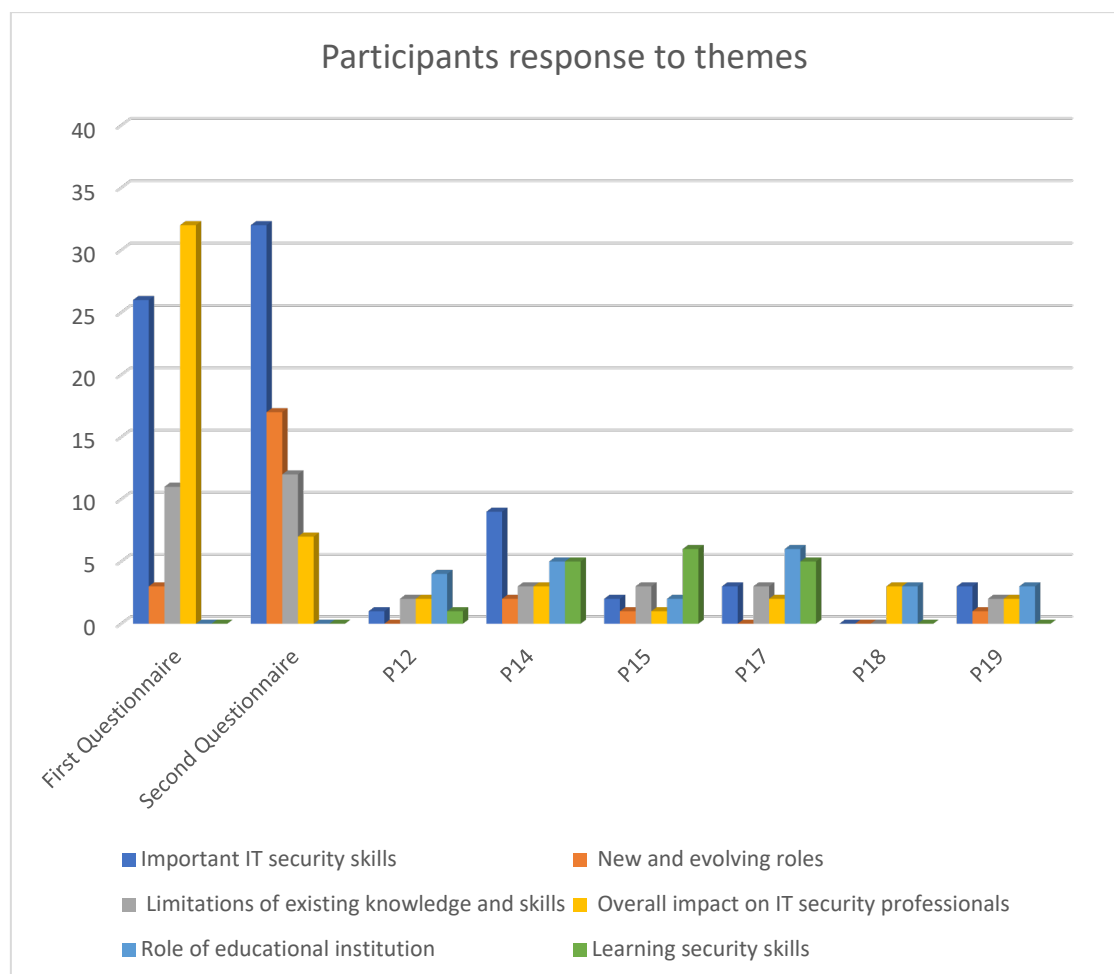


Figure 4.9: Summary of Participants Response to Themes

4.3 THEME ONE – IMPORTANT SKILLS

The first theme that emerged is the important skills required to cope in the Cloud environment. This theme is in line with the first research question, which seeks to elucidate the important skills required by IT security professionals to cope with Cloud computing technology. These skills are categorized into technical and non-technical skills. Figure 4.10 provides an overview of participant's responses to the important skills.

4.3.1 Technical Skills

Most of the identified skills are technical skills. While the skills required by IT professionals might be changing, the technical skills are still deemed very important in managing and working in Cloud environments.

4.3.1.1 Basic IT skills

The first subtheme in the technical skills category is basic IT skills. Participants believe the basic IT skills are still important and fundamental in working in a Cloud environment. Overall, there is much emphasis on programming skills in this category. The participants note that with a rise in automation, there is going to be a rise in the need for programmers in the future. Participant 12 says:

“definitely for things to get automated, you need programmers to write the code.”.

Other skills included in this category are service and traffic management. For example, participant 12 and 14 notes that

“well, I still think the core skills of IT is still needed in terms of you know, in terms of scripting, patching, and all those kind of things.”

“Python is really brilliant for security people. It's always good to understand programming language even if it's basic. It's good to understand the basics of coding. Sometimes for a security person, you want to see a code someone has deployed into the Cloud; it's not a problem because when you deploy code into

Cloud and it has a problem, you want to make sure code is secured and everything is right in place.”

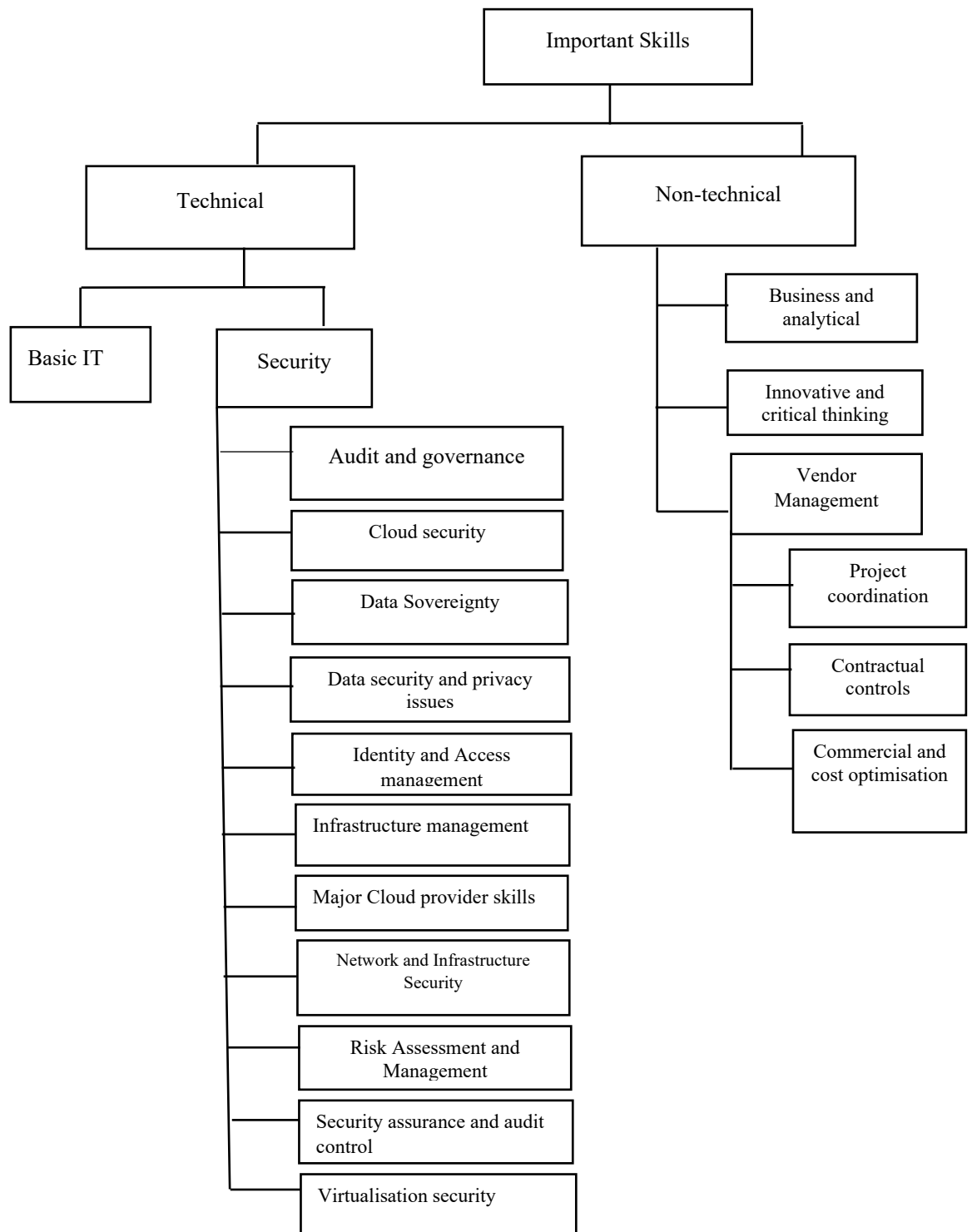


Figure 4.10: The Overview of Codes For Theme One

4.3.1.2 Security

Security is an all-encompassing word used by the participants throughout data collection. There is a large focus on risk assessment and management of risk, and management in the security category. An overarching skill requirement by most of the respondents is that there is a high requirement for skills around risk assessment and leadership in the Cloud environment. Cloud technology increases the attack surface and makes risk management a difficult task to achieve. The following excerpts illustrate some of the participant's views on the need for risk management skills.

*“Significantly increased the need for formal risk management training”,
“You still have to have a full-stack understanding in order to assess risks exposed, maybe at not at quite the depth on physical security aspects but this still comes into play for the consumers of the Cloud service and the devices that they use. The data is still held somewhere in something that has a level of risk that you need to understand.” “This is one area where most change will take place. A much larger amount of data will be travelling out of our network boundaries, mobile apps are on the increase, and people are working from a remote location. Securing our data will become increasingly more difficult.”*

Identity and Access Management (IAM) is another prevalent skill in this category. IAM provides a means of authentication and authorization in the Cloud. Cloud shifts the focus to remote and external access, which attracts attackers and hackers. Therefore, having identity and access control in the context of the Cloud is deemed important. One of the participants reveals:

“the most important skills you’ll have is access management is very important in this area”

Furthermore, Cloud security skills are identified as one of the security skills. Participants say that it is important to understand the architecture and security of Cloud computing to thrive in the Cloud environment as IT security personnel. For example, one of the respondents says, *“Firstly, understanding of Cloud architecture and how it works, then understanding the security from the Cloud perspective.”*. It recommends

that training with major Cloud providers could facilitate this understanding. Another skill group that emerged is data sovereignty, data security, and privacy.

“There are a number of new things to think about, such as data sovereignty and laws required to operate in data centers which aren't always in the same country you would have hosted before.” “data sovereignty and global privacy issues are now needed to ensure all risks are covered.”

Cloud services, especially data storage, are breaking the traditional geopolitical barriers of data privacy, and so skills around understanding legal requirements and compliance of data to enforce global data privacy are necessary. Other skills identified in the security category are information security governance and audit controls, virtualisation security, and network and infrastructure. Network and infrastructure security skills are essential to protect and manage the organisation’s Cloud infrastructure –

“So, infrastructure management means that you understand, you understand the company, the basic components that make the Cloud platform, you understand the commercial part as well which might seem not technical but it’s very very important.”

Also, participants add that migrating to the Cloud could sometimes imply security and compliance issues for businesses as auditing and governance in the Cloud could be complex. There is still a gap in how to measure performance and risk. Also, a new strategy is needed on how to govern and audit IT resources and people to align with business objectives. Participant P15 says regarding audit controls:

“We used to go physically and actually audit controls, but you can't ring AWS and say hey, I want to go and have a look at your physical security in your data centres now.” Furthermore, “Having advanced skillset of virtualisation security is a must, and this can be applied to a various set of Cloud services. Also, the usual security principles still apply to the Cloud”

4.3.2 Non-technical Skills

Four skills that emerged in this category are business and analytical, innovative and critical thinking, and vendor management skills. There is a shift in IT professionals focusing on business and analytical skills. Innovative and creative thinking is necessary

for professionals to view and address security in light of Cloud technology. Participant P01 says:

“As a general rule though for ALL staff, developing a new thinking pattern is absolutely critical. Incorporating all the key areas of thinking is important to deliver a secure product. Too often, it's a "just make it work" mentality that leads to issues in Security, gaps in risk controls, and over-provisioned environments. As an example, trying to educate teams to ensure they understand THEY own the risk for their systems and not the risk teams have been a huge challenge. It requires a shift in thinking to really take accountability for what they build”.

“Cloud technology is requiring new thinking patterns and is currently lacking people with critical thinking that can cover a lot of those domains.”

Furthermore, vendor management skills are highlighted as important. There is an emphasis on commercial and cost management, contract negotiation and controls, and project coordination/management. Participant P17 says commercial cost optimisation is in high demand as an organisation creates roles around managing cost.

“A lot of organisations now are creating teams around managing their cost in the Cloud, because most of the Cloud services they charge you per hour of using the services, some even charge you per minute. There's a high probability that some services are in use but not in use, and you just deploy them, nobody is using them, and they are incurring the cost for you. So, if you learn to manage those commercial aspects of Cloud is another good skill”

The fourth non-technical skill that emerged is the contractual controls. The skills around understanding contractual agreements and negotiating skills. Participant P14 says,

“So there are some things we do in the Cloud, you will go through some service provider, they will just ask for the requirement, negotiate the deal, the money for the contract, how much do you want us to pay, how much will be charged per annum for hosting this mail, things like that. So, all those things are still skills that are required.”

4.4 THEME TWO – EVOLVING AND NEW ROLES

The second theme that emerged from the data is changing and new roles. These changes have significantly affected the services, skills, and responsibilities of IT personnel. The traditional role of IT in an organisation includes maintenance of corporate infrastructure, updating systems, as well as providing support. The IT department recruits IT, professionals, such as systems administrators, developers, and IT support technicians, to perform these tasks. Evolving roles are dependent upon the business strategy and the Cloud service being consumed by the organisation. Most of the participants advise that roles involving infrastructure and network management changing in the Cloud. Also, the data reveals that application developers need to upskill or risk getting made redundant:

“Most of them especially the one relevant to infrastructure and network, even application development to some extent.”

Also, the data reveals that system support personnel are going to be reduced as their services are no longer required.

“Less personal are needed in certain areas. 1. People who manage servers. 2. Software licencing. 3. day-to-day operations. In some areas, the personnel will need to upskill to Cloud-based skills”.

“in relation to the hardware installation component, it is no longer relevant as you are effectively subscribing to a service. For a full as a service model, security is also taken care of”.

While the Cloud is reducing and changing job roles, it also creates new roles. For example, participant 19 says that while job roles around physical, infrastructure and network security and management may be evolving, organisations also needs Cloud architects to develop their Cloud strategy and manage the Cloud architecture. Also, the roles of security architects, Information security analysts, and configuration management are becoming popular and important with the Cloud.

“You won't be needing this, but it doesn't necessarily mean that you're actually eliminating all those people, you will have to have Cloud Architects, Cloud people who can work on the Cloud data.”

“The roles such as server engineer or admin is basically going to cease to exist, but roles like configuration management only are becoming Tier 1 roles where they previously, they weren't”

4.5 THEME THREE – CHALLENGES FOR TRADITIONAL SKILLS

Theme three captures some of the challenges for the traditional skill sets, highlighted by the participants. Three sub-themes emerged in this category: a need for broader knowledge, traditional skills are not so relevant, and proprietorship makes acquiring Cloud skills difficult. Considering that Cloud has increased the attack surface, and so professionals need to think and manage risk on a global level. Participants suggest that IT security professionals have a broad knowledge of cybersecurity skills.

“Currently it is very difficult to find people with broad enough knowledge of cybersecurity to ensure that all levels of risks are understood and presented to the business owner. This is not just limited to Cloud computing.”

“Finding people or/and cost-effective security services with sufficient depth of knowledge and experience to understand, end to end development pipelines, full-stack solutions and automation skills to efficiently and accurately assess the security risks is a key challenge.”

Apart from the greater emphasis on having a broad Cloud knowledge and skills set, the data reveals that traditional skills are not so relevant working in the Cloud. Cloud, like every other technology, requires specific skills that require upskilling and training for staff or organisations when getting competent staff. Two of the participant's notes:

“It's important to keep relevant with industry technologies. Cloud is no exception. While the concept of Cloud (essentially co-hosting) is not new, the platform that overlays the hosting is what matters most and requires new skills to understand and leverage the interfaces.”

“Simply put, if you don't have the specific skill, you won't be able to compete, let alone applying for relevant jobs.”.

Also, because roles and responsibilities are changing, it requires a new set of skills as some might be irrelevant. For example,

“With the development of Cloud technology, a lot of changes will come into place, and therefore, the roles and responsibilities of IT professionals will change to an extent. Obviously, the Cloud is not the same as your traditional on-premise database”,

“it’s a new role; it requires new skills because it’s a new definition of the Job description.”

“There are always going to be some irrelevant skills that you used before that won’t be needed now. I.e., if you go from Vmware to Azure, your Vmware specific knowledge isn’t likely to be useful. However, general concepts, etc. may still be.”.

Participants also emphasized that the type of Cloud service and organisation is consuming determines the required skills. They believe when an organisation is planning to adopt Cloud computing, the skills required for the Cloud service should also be considered.

“Depending on the Cloud service (IaaS, PaaS, SaaS etc) and deployment (Private, Public, Hybrid etc) models, specific skillsets and knowledge may be required. ”

“You need to understand what services you are subscribing to in order to assess the security posture and apply the appropriate controls ”

“although there are similarities but with different types of Clouds and Clouds services, providers tend to somehow makes skillset unique to their service hence the certification trend as an acknowledgment of knowing.”

Another challenge that emerged from the data is the issue of the proprietary nature of various Cloud providers. New job responsibilities require a new set of skills, and the issue of proprietorship makes it difficult for professionals to decide which skill should be learned. One of the participants reveals that you have to get skilled in the product or service you are using.

“However, where the problem is, I think is the issue of proprietorship which you have AWS on one side which is amazon and Microsoft at the other end who are the big players in the market. So, that is where the problem is where this professional has to learn and choose a side. It is quite rear for you to find

someone with Amazon qualifications and Microsoft, and all that is where the problem is. So, you still need the basic skills, and you still need to learn how it works with Amazon, or you know how it obviously works differently with Microsoft. It still needs a bit of upskilling in terms of the product you are getting. For example, I have a bit of a problem at the moment; I am training for AWS and all that, but then automatically, if you go on to search job, you see automatically once I see something that has to do with Azure, I say no this is not for me. So, you see, already, because of the divide in the market, and I will say you see it's not standardized. So, it makes it hard."

4.6 THEME FOUR – OTHER IMPACT

Theme four is around findings on the other impacts Cloud is having on organisations that are directly or indirectly related to skills and roles. Three sub-themes emerged: Cost management, Enhanced security, and Focus on business core

4.6.1 Direct Skills and Roles' Impact

The findings reveal that the Cloud is causing a major restructuring in user organisations. It is changing the way people work and what job needs to be done. Cloud is introducing new threats that affect the established business model, and the overall staffing model is affected. Two categories emerged from this theme: New skillsets, and firing and hiring.

4.6.1.1 New skillset

There is a high consensus on the need to upskill to stay relevant in the industry. Different new skills set are required to be able to manage Cloud services. The jobs and skills have been fundamentally transformed. There is an ongoing redefinition of skills and job roles. Participant P01 says:

"New skills are definitely required - I myself am going through AWS training (Cloud Practitioner) and have been through Azure AZ100. It depends on the level of operation you will be performing in the Cloud as to what skills you'll require."

Also, there is also much emphasis on industry certifications and training. As Cloud

skills are yet to be standardized and are proprietary-based. Most organisations are having to train their employees on how to use the Cloud platform.

“Yeah, I mean, I think Cloud computing is changing the way we work. It's changing the way IT operations are managed, so you know from the dynamic skill sets to changing skill sets and the fact that services are being migrated to the Cloud. The fact that slightly different organisational skill is required to be able to be able to manage services in the Cloud, that is a huge change by itself for individuals and organisations.”

“ That’s why you need to go for certifications, train yourself more, and have a full view understanding of these things. You know that’s why in the real industry, specialist industries like security, when they put a job, they always put there that this will be an added value if you have like additional requirement like CISM, CISSP or CISA all those things. You are going through those things, and trying to find yourself, it means you have to go through a different understanding of them.”

“A lot of these skills for Amazon or like AWS. Potentially I would say this. Aws or Azure experience will count in terms of how we might hire. So, if someone is very experienced in Azure, it wouldn't necessarily be a problem that we would probably prefer someone with AWS experience because the models as much as they are similar, being like certified in one of the AWS foundational courses might be better.”

4.6.1.2 Firing and hiring

As the business model shifts, there has also been some restructuring, redefinition, and redistribution of IT roles and responsibilities, and some roles are gradually becoming redundant. IT roles are shifting into a more business-focused position, from adhering to a process that is supported by technology to managing a technology-driven process.

“Security roles are having to adapt new methods of testing, assessment, and setting frameworks to allow staff to move within the guidelines.”

“Current IT security practitioners are forced to adapt their skills into new environments, and to emphasize those skills on principles as opposed to technologies.”

“More of an awareness perspective as to who is doing what in terms of the Cloud provider. Security roles will eventually become more of a governance role as opposed to one of “doing.”

“I believe in 5-7 years’ time we won't recognise our departments anymore. New skill set, new ways of working, and new job titles.”

“...and organisations to focus on training or hiring new staff.”

“cut jobs in some cases given most organisations would have less need for on-premise IT Security Engineers etc.”

Some roles are being made redundant as organisations consume Cloud services. This results in firing some employees while some new roles are being created. IT security professionals are required to adapt their skills to the new environment. Additionally, some of the participants believe the Cloud is enhancing a lot of task automation, which may lead to lesser staff.

“With Cloud came a lot of automation talk, because you can programmatically interact with Cloud services for provisioning, de-provisioning, configuration change, and deployments. This isn't fully attributed to the Cloud, but Cloud drove a lot of adoption of the thinking because it provided the avenues required to allow automation, whereas a lot of traditional on-prem platforms weren't capable of such automation.”

“Yes, a lot of services/applications are being automated, so need for only lesser IT staff.”

4.6.2 Indirect Skills and Roles’ Impact

The results show other impacts of Cloud computing aside from its effect on skills and roles. The following sub-sections review the responses on the impacts of Cloud services adoption not directly related to skills and roles.

4.6.2.1 Cost Management

The data reveals that the Cloud provides some form of cost advantages to businesses especially in the area of reducing people and infrastructure costs. Cloud is moving from

CAPEX (capital expenditure) to OPEX (operating expenditure). Outsourcing of services and functions to CSPs provides opportunities to manage costs efficiently and, overall, increasing workforce productivity. Personnel can focus on strategy and innovation.

“With the adoption of the Cloud, there is a gradual drive towards the reduction of OPEX (people cost) ”

“Saving the business a lot of money in terms of paying staff to maintain systems and servers, upgrade hardware (costly), and salaries.”

4.6.2.2 Enhance security

Most participants reveal that the Cloud provides the opportunity to enhance security. At the same time, there is a consensus that using the Cloud does not correspond to enhanced security. However, the data reveals that Cloud does provide the security apparatus for its products. Still, it depends on the user organisation’s strategy and contracts to configure these products to suit their security needs. Participant 15 agrees that the Cloud does position the organisation for enhanced IT security.

“Absolutely, pretty much. So, moving into Cloud gives you an opportunity to be reactive and basically uplift your security posture.”

There is a greater emphasis on the adoption of security techniques. Participant P19 says the Cloud has improved tools and processes to implement security features.

“ positive thing that in terms of security with the Cloud is I mean everyone is actually forced to use a particular set of security strategy that the Cloud provider use for example, in Azure if you host your let's say a virtual machine is your they have got a basic set of security rules that you're forced on to use that No one can come on access it within the infrastructure. ”

Depending on the type of service and contract agreement, the Cloud provider could be solely responsible for providing the security, or it could be a shared responsibility between them and the user organisation, and sometimes the user organisation could be responsible for their security. Also, participant P12 reveals that the Cloud provides physical security because the Cloud removes the need for in-house infrastructure security.

“In terms of Availability of IT resources, for example, IT security pros will

largely consider physical security of their resources. Cloud changes/reduces that”

4.6.2.3 Focus on business core

As services are being outsourced to the Cloud, business employees can focus mainly on the core of the business. Adopting the Cloud has reduced the need for infrastructure maintenance by the IT team; therefore, they can focus more on business strategy and innovation. One of the participants adds:

“With the adoption of Cloud, there is a gradual drive towards the reduction of OPEX (people cost), saving the business a lot of money in terms of paying staff to maintain systems and servers, upgrade hardware (costly), and salaries.”

“once you have moved to the Cloud, you can move more to have your full-time employees as that working on your core service of the business. So, if your if your core Services the business is to provide SAP or your core is to provide a security tool managing data center. You wouldn't necessarily need people to manage that because, again, your responsibility has now changed. So, it allows you to have your immediate staff compliment is closer to actually what your core product is rather than having quite a large set of tasks.”

4.8 THEME FIVE– ROLE OF THE HEI

There is a consensus from 80% of the participants around the role of the HEI and industry bodies in filling the skills gap. Most of the participants believe the university needs to review its curriculum for teaching fundamental technical concepts to capture the relevant technology and security skills required. They suggest the University is not preparing the graduates with the right skills for the labour force. They also reveal the rapid change in technology, such as Cloud computing, is generally changing IT. Fundamental courses like software development are also changing, and these changes should be effected in the curriculum.

“They just need to adjust. I will give you an example, the CISSP certification is a security certification right. I will tell you about three years ago, their certification domain, so they have like 8-10 domains for studying for the exam,

they didn't include anything about the Cloud at all, even though it's not Cloud-specific, they still have CCSP right, but CCSP was just about security, about compliance, about regulatory, risk management and the rest. And then, they've readjusted it now, they've added some new topics into those domains, and there's a Cloud in there. Not really deep, but at least the beginning, it talks about regulatory, how it works, and you know security around it. But it's very important, but I think it's that same way that that should operate in an academic environment and educational institutions."

Furthermore, P12 adds that schools should incorporate some of the curricula of the big players in the market to increase graduates' employability and bridge the skills gap. The participant says that this is similar to how the CCNA course is been taught as networking fundamentals in some schools.

"The core IT skills are essential, you can do without them, but then at some point in time if possible, introduce the student ehm to the products, to the ones who are leading the market, AWS, IBM, AND ALL THAT. So, maybe one or two courses or three, depending on they want them but I think it's really important because that what the recruiters, the employers, companies are looking for. That's what they use directly. So, when the students are skilled in that, then obviously, it's quite easy, they are coming out with two how do I put it? With two strongholds, in terms of IT and then one of the vendors or two of the vendors, maybe. Ehn the school institution, I was quite fortunate. I went to ..I did a postgrad that was based on Cisco products, so that really helped me and catapulted me into the job and getting a job in New Zealand whatever. I didn't have that in New Zealand. It's in another country. But then, that advantage gave me that confidence because I've played with those products during my university days, so it made it more easier for me to work with the system."

While most of the participants believe the school curriculum should be updated to align with the overall changes the Cloud is bringing, participant P17 recommends schools should only teach the fundamental changes happening at the core lower layer because the higher-level skills can be easily picked up. Changing a curriculum to include high-level skills that are continually evolving will not be advisable.

“Like I said earlier, the way these things keep changing. I don’t think it right for educational institutions to change their curriculum. What’s Cloud? what does it mean to host a Cloud or create Cloud service? Maybe that one can be taught but not those upper layers, maybe the lower layer can be taught like the aspects of the Cloud, where the Cloud is used, and all that because all of them are similar technology specialization. The utilisation of the software, settings and things like that. So, I believe those ones should be taught. It will add more value if they are taught in school. I mean, there’s no point learning how to configure MySQL in the Cloud. You can pick up that, but you should learn what Cloud services are about. You should understand what Cloud technology is about because if you understand what Cloud technology is about, the underlying layout, virtualisation, and how to program it, how to configure it. Yes, that can be taught in school.”

However, participant P17 reveals that Universities should be careful and proactive about these changes. They need to lead the change and not be bought by some providers.

“I do think that if the university is not leading, they would be bought by the big players in the Cloud.”

There is also an emphasis on how industry security bodies such as ISC² and ISACA constantly review their curriculums to effect changes. The data also reveals that the skills you are equipped with from the higher institution are not expected to be enough to get you going in the market. You’ll need industry training and certifications as they have more compact courses that are detailed to acquire security skills. Organisations can arrange for training and boot camps, but a lot of work is still on the individual.

“So ISACA, for example, will teach all this course which is ehmm you know CISA and that is part of their Frameworks, and they tend to be more very compact courses, but they actually require with new high knowledge for you to start.”

“They just give you everything, there is a curriculum; they will just skip through the information you need to know at the surface. So, going in-depth is going to all those special specialties itself like security specialty. If you want to be really

committed, you go for something like what is it called PMP, project management. You'll deal with real core project management. So, you can't really get like all, and you can't get 100% from the uni."

"Ah! Well, it's still a bit tricky. I think the basics of IT can be taught in a normal traditional way of schooling, but then the issue of proprietorship, which obviously is quite hard to teach you to know ehm in a university setting. Individuals who've got the basics, who have gone through the rudiments of IT can easily learn on their own, which is what I'm doing at the moment. Pick up Cloud computing; you know they can actually do it. We did a little bit of those in my current work, but then it quite diverse it's hard to say who learns this in the classroom. You learn as it comes."

4.9 THEME SIX – LEARNING SECURITY SKILLS

This theme emerged on where and how practical security skills can be learned. The result shows that security should be an advanced level qualification. Participant PI4 and P15 believe security should be an advanced course and should not be a core degree course. Security is the top layer of core technical IT skills.

"I don't believe anyone should be doing security as a primary, like an undergraduate type of course. Like some of the best security, people don't have technical degrees as well. So so they've come from like philosophy majors or something like that. They've not necessarily done engineering. Ehm so so like one of the companies I consult to, the governance manager there is, he has a master's in Philosophy, for example, another one of the organisation's I deal with, the head of security is actually a lawyer by trade. so people for... I believe that the undergraduate degrees should be like one of the domains type things if you're going to do a graduate degree get some experience in that and then move into security because you'll be much better security professional for that"

"security skills usually require people to go out and train. You know we have courses like CISSP, CISM, then you may want to actually go for a bootcamp or something like a training. 1-week training, two weeks training whatever or sit

down and study and then do some online courses or watch their video or whatever.”

Furthermore, the data shows that the security skills needed for the Cloud are best to be acquired in an informal environment rather than in a traditional school setting. Professional bodies have a more compact curriculum, and going through such trainings increases your marketability and validates your skills rather than only a University degree.

“I will tell you that employer will prefer to pick someone with that certification like CISSP and all the rest before even thinking of someone with only a bachelors. Because they believe Bachelor is just a scratch on the surface, but certifications are tuned for personal growth so that the way they look at it in the area of security as well as other personal areas as well because it’s stronger. They believe you have the real professional understanding of how things work.”

It reveals that the way the current University curriculums are designed, they are teaching the concepts, and that is why you still need to go through the industry bodies to get the core skills. The University only teaches you the concepts which may not be enough to get you a job.

“They just give you everything; there is a curriculum; they will just skip through the information you need to know at the surface. So, going in-depth is going to all those special specialties itself like security specialty. If you want to be really committed, you go for something like what is it called PMP, project management. You’ll deal with real core project management. So, you can’t really get like all; you can’t get 100% from the uni.”

“You can only teach what is standardized, so that’s when you can bring it into the traditional ehmm...If anyone is actually going to do a 4-year degree in Cloud, I will be like do you have to? It kind of limits and restrict you in a way from my own perspective anyway. I would rather learn the core protocols of technologies standardized in the university; then, probably, Universities can say Ok cool. You may want to a course in AWS or Microsoft or choose from

maybe. I look at the core IT skills as the cake and the proprietorship in terms of Azure Microsoft, AWS, or whatever it is as the icing.”

4.10 DOCUMENT ANALYSIS RESULTS

The analysis shows that the majority of the universities do not offer cybersecurity or Information security programs for undergraduate degrees. Table 4.8 shows that most of the universities however allow students to major in security programs with a few additional security courses from computer science or engineering programs. The percentage of security exposure is low and most of the security courses are elective which means it is possible not to take the courses. Victoria University is the only school that offers a cybersecurity Engineering degree program. Even with a security program, the security courses' point value is less than one-third of the total points required for the program. Also, Victoria University is the only school offering a clearly defined Cloud course. None of the schools has a Cloud degree nor course. It is noteworthy to mention that the University of Canterbury offers a course on Big data computing and systems where they introduce students to the fundamentals of Cloud computing. The course provides students skills in distributed computational techniques, distributed algorithms, and systems/programming support for large-scale processing of data.

With the demands to close the skills gap in the cybersecurity workforce, the university's undergraduate curriculum is not doing enough to prepare the students for the workforce. Overall, the result as shown in Table 4.8 shows that the Universities are not yet taking the lead in implementing the required changes to meet the ever-changing demands of the industry.

Table 4.8: Analysis of Undergraduate Programs in Selected New Zealand Universities

University	Program	Course		Note
		Security-related	Cloud	
University of Auckland (University of Auckland, n.d.)	B.Sc. in Information and Technology Management	Information Security in Business (Elective)		There is no undergraduate security or Cloud Program at the University of Auckland. However, there are more detailed postgraduate security programs. The B.Sc. in Information and Technology Management includes a course on information security which provides students with knowledge of activities, methods, and procedures used by businesses to establish robust information security policies. The security course

	(BAdvSci(Hons)) in Computer Science (University of Auckland, n.d.)	Cyber Security (Elective) Security for Smart Devices (Elective) System Security (Elective) Network Defence and Countermeasu res (Elective) Cryptographic Management (Elective)		only covers 15points out of the 360 point program. Similarly, the bachelor of advanced science in computer science includes five elective security courses that the students may choose from. These courses make a 15.6 % of the points required for the program should a student choose to focus on security.
University of Otago (University of Otago, n.d.)	BSc Computer Science Honors	Cryptography and Security (Elective)	Cloud Computing Architecture (Elective)	The University of Otago does not have an undergraduate program in cybersecurity or Cloud computing. However, Computer Science majors have the opportunity to choose elective

	Bachelor of Applied Science (BappSc) Majoring in Software Engineering (Hons)	Cloud Computing Architecture Cryptography and Security (Elective)		security and Cloud course. Cloud computing introduces the students to fundamental technologies used by Cloud computing providers to build their platforms
AUT (Auckland University of Technology, n.d.)	B.Sc Computer and Information Science (Network and CyberSecurity Major)	Network Security Advanced Network Technologies (Elective) Enterprise Networks (Elective) Highly Secure Systems (Elective) Information Security Management (Elective)		A total of three security courses are taken to major in Network and CyberSecurity. The security course only takes 12.5% of the total course requirement. Network security covers LAN, WAN, and Wireless security focusing on the functionality available and configuration of network and link layers. The highly secure systems Provide an in-depth understanding

				of LAN, WAN, and Wireless security focusing on the functionality available and configuration of network and link layers.
University of Canterbury (University of Canterbury, n.d.)	B.Eng software Engineering with Honors (University of Canterbury, n.d.)	Data and Network Security		The Software Engineering program includes a security course on Fundamental principles of computer and network security which introduces the students to securing information at rest, during transmission, and information stored on the network
	B.Eng Comp Engineering Honours	Discrete Mathematics and Cryptography (Elective)		There is an option of taking Discrete Mathematics and Cryptography. The course introduces the students to

				<p>graph theory and cryptography. That's 8.3% of the points required for the Computer Science program</p>
	<p>BSc Computer Science Major (University of Canterbury, n.d.)</p>	<p>Data and Network Security</p> <p>Secure Software (Elective)</p>	<p>Big Data Computing and Systems</p>	<p>The secure software course provides students with skills to design and implement secure application programs, which are not vulnerable to malicious attacks.</p> <p>The course teaches the fundamentals of Cloud computing. It provides students skills in distributed computational techniques, distributed algorithms, and systems/programming support for large-scale processing of data.</p>

University of Waikato (University of Waikato, n.d.)	B.Sc Computer Science	<p>Practical Networking and Cyber Security</p> <p>Advanced Networking and Cyber Security (Elective)</p>		<p>The University of Waikato does not offer security nor Cloud degree program. It includes a course that provides an overview of the technologies and protocols involved in computer communications and cybersecurity.</p>
	B.Eng Software Engineering Honors	<p>Practical Networking and Cyber Security</p> <p>Advanced Networking and Cyber Security (Elective)</p> <p>Cryptography and Number Theory (Elective)</p> <p>Malware Analysis and Penetration Testing (Elective)</p>		<p>If a student selects all the elective security courses in the course of the program, the security courses constitute 12.5% of the points required for the program</p>

		Cryptography (Elective) Human and 149irtualizatio n security (Elective) Clouds and Networking (Elective)		required for the program
Massey University (Massey University, n.d.)	Bachelor of Information Sciences (Information Technology) (Massey University, n.d.)	Technology Governance and Risk Management Networks, Security and, Privacy		Massey University does not offer a security nor Cloud degree. However, it includes 2 security courses which make 8.3 % points of the total points required for the program.

Professional certification offers a more comprehensive security curriculum as can be seen in table 4.9. The vendor-neutral Cloud certifications provide the fundamental skills and expertise required to securely provision and manage Cloud computing while vendor-specific certificates provide insights into a particular product. The result shows that unlike the Universities, most of the domains are updated as the demands for the industry change. Cisco for example, just included Cloud certification as the big companies migrated to the Cloud. The required skills for managing Cisco products in the Cloud are different, hence, the need for a new certification. While there are many vendor-specific certifications such as Microsoft and Amazon which have several Cloud-based certifications, this analysis selected Cisco to capture the changes in the

skills required before and after migrating to the Cloud. CCNA Cloud certification is job-role-focused. It is used to validate skills for Cloud engineers, Cloud Administrators, and network engineers that provision Cisco products over the Cloud (Cisco, n.d.). This information is important to demonstrate the changing industry skills and role requirements.

Table 4.9: Analysis of Professional Security and Cloud Certificates

Professional Body	Curriculum
Vendor-Neutral	
Cloud Security Alliance (CSA) (Alliance, n.d.)	<p>1. Certificate of Cloud Auditing Knowledge (CCAK) is being developed by CSA and ISACA</p> <p>The domains are yet to be known. The CCAK tests the knowledge in the essential principles of auditing Cloud computing systems</p> <p>2. Certified Cloud Security Knowledge (CCSK)</p> <p>The CCSK has 14 knowledge domains:</p> <ul style="list-style-type: none"> i. Cloud Architecture ii. Governance and Enterprise Risk Management iii. Legal Issues, Contracts, and Electronic Discovery iv. Compliance and Audit Management v. Information Management and Data Security vi. Interoperability and Portability vii. Traditional Security, Business Continuity and Disaster Recovery viii. Data Center Operations ix. Incident Response x. Application Security xi. Encryption and Key Management xii. Identity, Entitlement, and Access Management xiii. Virtualisation xiv. Security as a Service
Information Systems Audit and Control Association (ISACA)	<p>1. Certified Information Systems Auditor(CISA). The CISA has five domains (ISACA, n.d.):</p> <ul style="list-style-type: none"> i. Information Systems Auditing Process

	<ul style="list-style-type: none"> ii. Governance And Management of IT iii. Information Systems Acquisition, Development, And Implementation iv. Information Systems Operations And Business Resilience v. Protection of Information Assets <p>2. Certified in Risk and Information Systems (CRISC). The CRISC has four domains (ISACA, n.d.):</p> <ul style="list-style-type: none"> i. IT Risk Identification ii. IT Risk Assessment i. Risk Response And Mitigation ii. Risk And Control Monitoring And Reporting <p>3. Control Certified Information Security Manager(CISM). The CISM test for expertise in four domains (ISACA, n.d.):</p> <ul style="list-style-type: none"> i. Information Security Governance ii. Information Risk Management iii. Information Security Program Development & Management iv. Information Security Incident Management
The International Information System Security Certification Consortium (ISC2)	<p>1. Certified Information Systems Security Professional (CISSP). The CISSP includes eight knowledge domains (ISC2, 2020)</p> <ul style="list-style-type: none"> i. Introduction to Security and Risk Management ii. Asset Security iii. Security Architecture and Engineering iv. Communication and Network Security v. Identity and Access Management (IAM) vi. Security Assessment and Testing vii. Security Operations viii. Software Development Security <p>2. Certified Cloud Security Professional (CCSP) The CCSP includes six knowledge domains (ISC2, n.d.):</p> <ul style="list-style-type: none"> i. Cloud Concepts, Architecture and Design ii. Cloud Data Security iii. Cloud Platform & Infrastructure Security iv. Cloud Application Security v. Cloud Security Operations vi. Legal, Risk, and Compliance

	<p>3. The Systems Security Certified Practitioner (SSCP). The SSCP has seven knowledge domains:</p> <ul style="list-style-type: none"> i. Access Controls ii. Security Operations and Administration iii. Risk Identification, Monitoring, and Analysis iv. Incident Response and Recovery v. Cryptography vi. Network and Communications Security vii. Systems and Application Security
CompTIA	<p>1. The Cloud + includes five domains of expertise (CompTIA, 2019):</p> <ul style="list-style-type: none"> i. Cloud Architecture and Design 13% ii. Security 20% iii. Deployment 23% iv. Operations and Support 22% v. Troubleshooting 22% <p>2. CompTIA Security + The security+ certification includes five domains (Lane, 2020):</p> <ul style="list-style-type: none"> i. Attacks, Threats, and Vulnerabilities (24%) ii. Architecture and Design (21%) iii. Implementation (25%) iv. Operations and Incident Response (16%) v. Governance, Risk, and Compliance (14%)
Vendor-Specific	
Cisco	<p>1. CCNA Cloud The CCNA Cloud includes two exams.</p> <ul style="list-style-type: none"> i. Cloud Administration (CLDADM). It includes three domains (Cisco, n.d.): <ul style="list-style-type: none"> • Cloud provisioning, management • monitoring, reporting, • Charge-back models and remediation. ii. Cisco Cloud Fundamentals (CLDFND). It includes three domains: <ul style="list-style-type: none"> • Unified Compute including Cisco UCS and server virtualization • Unified Fabric including DC network architecture and infrastructure virtualization, and

	<ul style="list-style-type: none"> • Unified Storage including integrated infrastructure solutions <p>2. CCNP Cloud</p> <p>The CCNP Cloud has four exams (Cisco, n.d.):</p> <ol style="list-style-type: none"> Implementing and Troubleshooting the Cisco Cloud Infrastructure (CLDINF). It includes the following domains: <ul style="list-style-type: none"> • setup Cloud infrastructure including physical and virtual Data Centers • implement Storage infrastructure and connectivity • implement Network infrastructure and connectivity • implement Compute • troubleshoot Cloud workflows or applications • identify infrastructure operational domains Designing the Cisco Cloud (CLDDDES). It includes the following domains: <ul style="list-style-type: none"> • translate requirements into Cloud/automation process designs • design Private Cloud infrastructures • design Public Cloud infrastructures • design Cloud Security Policies • design Virtualisation and Virtual Network Services Automating the Cisco Enterprise Cloud (CLDAUT) <ul style="list-style-type: none"> • Private IaaS • Private IaaS with Catalog Scaling • Private IaaS with Network Automation • Hybrid IaaS and • perform Application Provisioning & Life Cycle Management Building the Cisco Cloud with Application Centric Infrastructure (CLDACI)
--	--

	<ul style="list-style-type: none"> • ACI Architecture, Fabric and Physical Topology • ACI Design and Configuration • APIC Automation Using Northbound API • ACI Integration and • ACI Day 2 Operations
--	---

4.11 CONCLUSION

Chapter four presents the findings of the study. Six major themes related to the impact of Cloud computing on IT security skills and roles emerged from the data. Each of these themes is elaborated on with quotes from the participants. Also, the document analysis reported the readiness of certificates and degrees to communicate Cloud security information. Chapter five discusses the findings and the limitations, and implications for the study.

Chapter FIVE

Discussion and Implications

5.0 INTRODUCTION

The purpose of this study is to identify the impact Cloud computing is bringing on user organisations in terms of the necessary IT security skills, and changing roles. Chapter four has reported the findings of the research from the data collection techniques defined in Chapter three. The data is constructed to find meaningful patterns that would answer the research questions. Chapter five discusses these findings and provides a deeper analysis of the results in order to establish the meaning and contribution. It focuses on evaluating the findings and showing how the results relate to the literature and research questions. Overall, this chapter aims to provide a deeper understanding of the research problem through a logical synthesis of the findings.

Chapter five is structured to abstract the findings presented in Chapter four to highlight how the research questions are answered and the hypotheses formulated. Section 5.1 discusses the generation of hypotheses from the results that is critical for a qualitative process. It summarises the generation strategy and the processes applied. Section 5.2 describes how the research questions are answered with evidence from the results. Section 5.3 explains the triangulation of data collection methods. It provides details on how each data collection method contributed to the emergence of the themes in Section 4.2.4 in order to extend the interpretation and validity of the results. Section 5.4 discusses the findings in Chapter four. It relates the results with the literature to examine its relevance and implications. The significance of the results is found by referencing the literature. Section 5.5 concludes the Chapter with a link to Chapter six that summarises the research contribution.

5.1 GENERATING RESEARCH HYPOTHESIS

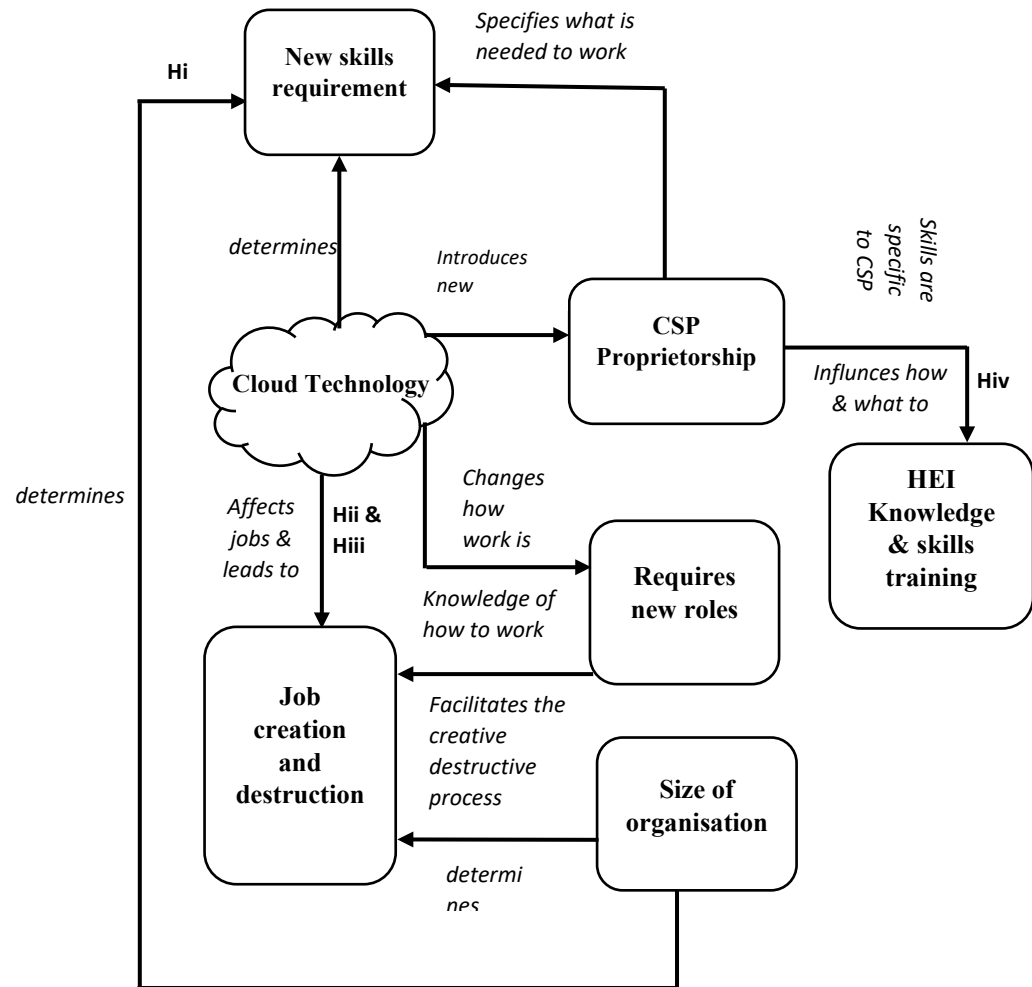
One of the main characteristics of qualitative research is theory/ hypothesis generation. A hypothesis is a tool for scientific observation (Casula, Rangarajan, & Shields, 2020, p. 5). They are falsifiable statements that are used to compare an expected outcome against the observed data (Darity, 2008). A hypothesis can be categorized into null/alternative, directional / non-directional, and inductive or deductive (Kabir, 2016, pp. 61-62). A null hypothesis is used to predict that there is no difference between the variables been studied while an alternate hypothesis predicts that there is a relationship between the variables studied. A direct hypothesis is used to predict the extent of the relationship between the variables studied while an indirect hypothesis only predicts that there is a relationship between two variables. In an inductive hypothesis, the researcher moves from specific expectations about individual occurrences to broader generalisations and theories while in a deductive hypothesis, the researcher moves from general theory to specific prediction (Soiferman, 2010, p. 7; Blackstone, 2018, p. 60). The aim of an inductive hypothesis is not to test the researcher's expectations or predictions against some empirical observations. Instead, it focuses on theory development or construction while a deductive hypothesis has the researcher's aim of testing observations made from theory (Blackstone, 2018).

While most qualitative studies are not designed for testing hypotheses, a qualitative hypothesis can be used to specify the tentative relationships between variables. It is possible to have an idea about possible answers to all aspects of the research questions. Chigbu (2019) claims that hypotheses are also applicable to qualitative research as qualitative studies can be inductive or deductive. However, unlike quantitative studies, it does not manipulate variables to isolate specific factors that are to be observed. Also, it is important to note that because of the relatively small sample size and the nature of the data in qualitative studies, using probability statistics for testing hypotheses is unnecessary. Qualitative and quantitative studies have different epistemological underpinnings and should be explained differently (2019, p. 8). A key difference between qualitative and quantitative research design is that research questions can be revised when necessary and hypotheses can be formulated after data has been collected. Also, a qualitative hypothesis tends to focus more on

necessary and sufficient conditions that would guarantee an effect rather than statements of correlation as in quantitative methods (Darity, 2008). Generally, quantitative methods are suitable for testing or validating the hypotheses that are generated from a qualitative study.

This Section discusses the formation of hypotheses. In this study, the problem is identified from the literature, then the population is selected and data is collected. In addition, the propositions are generated and hypotheses are refined. The research questions are used to guide and define the scope of the study for data collection and the research hypothesis is formulated based on the literature and the findings of the study and literature. The aim of these hypotheses is not for testing, but rather to generate meanings and develop explanations from the collected data. Figure 5.1 provides a schematic diagram for hypothesis generation, and Table 5.1 outlines the derived hypothesis.

Further to detailed data collection and analysis, four hypotheses are inductively generated. These are guided by the identified themes in the findings. As can be seen in Table 5.1, the categories of the hypothesis are direct, indirect, and inductive. It also outlines the data that generated the hypothesis. The data extra column has some of the extracts from the respondents' and participants' responses. The hypotheses are constructed from interpretations from the responses from the respondents and participants. Hypothesis i, ii and iii are generated from answering the research questions one, two, and three. The participants agree that the Cloud is generally causing a strong impact on IT security roles. Some roles are being automated and no longer required or reducing in number especially in support, and some new roles are being created. Hypothesis iv is generated from answering research question four. While most of the participants believe the higher institutions should facilitate teaching relevant security skills including Cloud skills, some participants believe Cloud technology is volatile and Universities should be strategic about how they handle changing their curriculums.



Keys

Hi: Hypothesis one Hii: Hypothesis two
Hiii: Hypothesis three Hiv: Hypothesis four
Hv: Hypothesis five HEI: Higher Educational Institution
CSP: Cloud Service Provider

Figure 5.1: Schematic Diagram for Hypothesis Generation

The first hypothesis is a general claim emerging from the results. This hypothesis can serve as a guide for further research. In addressing the impact of Cloud computing on the IT staffing model, the aspect of cost model, size, organisational strategy, job creation, and job destruction emerged. The first hypothesis addresses the cost model, strategy, and size of an organisation. Most of the respondents believe the cost model, size, and strategy of an organisation would determine the overall roles and skills

requirement. As seen in Figure 5.1, the size of an organisation to a large extent determines what skills are required. The skills and roles requirement for most organisations adopting Cloud require the size, cost model, and strategy of an organisation to determine what skills and roles are needed when migrating to the Cloud. The financial implication of adopting a particular type of Cloud or Cloud service might not be economically viable. The size and the financial status of an organisation determine which skills and roles to be migrated.

Table 5.1: Hypothesis Description

N0	Hypothesis	Category	Data Extract	Description
i	The size of an organisation and type of Cloud service determines the extent of the impact Cloud would have on IT security skills and job roles.	Indirect, Inductive	<p><i>“This is dependent on the extent of Cloud usage. Most of the infrastructure work will be taken care of by Cloud engineers. So staffing size of roles like network supports, infrastructure support might be shrinked. This is still due to the scale of any IT org. If scale is high, there's still need for infrastructure engineers and even network support to manage things like virtual Cloud etc.”</i></p> <p><i>“It also comes down to dollars as well; there are still cases where hosting on-prem is more cost-effective when you have scale and systems that may cost more to host in the Cloud. If there is an option for an org that has 20000 staff globally, chances are they have *significant* IT needs that could be met cost-effectively by owning their own data centers.”</i></p>	This suggests that new skill sets, both technical and non-technical skills are needed to work in the Cloud computing environment.

			<p><i>“Depends on your environment and cost models. For our environment, we are consuming much more SaaS rather than PaaS or IaaS. At this level identity and access are the key in-house security consideration, the rest of it falls into the contractual agreements, data sovereignty, and global privacy areas.”</i></p> <p><i>“I would say it's based on strategies that they use because when you move to Cloud the administration efforts become less so you can have the very least people on your team because every I mean, the data is all in one place. So when the data is in one place, it's easy to integrate from the I mean, you can integrate it wherever the data is because some Cloud and integrate them because the Cloud providers provide a medium such as APIs to share data between any applications. So, in that way I will say it's actually reduces Administration, right? So, we instead of having ten People in a team you can only have Five or six. So, the money that you save in you can actually put it on to Cloud to spend.”</i></p>	
ii	Cloud computing will create more new job roles than it destroyed in the IT workforce	Direct, inductive	<i>“you will have to have Cloud Architects Cloud people who can work on</i>	Working with Cloud computing technology will require new skills which would, in turn,

			<p><i>the Cloud data, so I would say”</i></p> <p><i>“Ehm, so, the core key skills needed at this point in time are predominantly DevOps type of skills. So so so in days gone by we used to like reckon stack servers now they are just all configurations code and infrastructure as code. So so coming from like a development background and moving into infrastructure one didn't used to be a thing but now it is. So you may start out of say a back-end developer and then move into to infrastructure as code type role.”</i></p> <p><i>“Like get the Cloud-based and all that. For instance, where I work, when we were migrating our server to the Cloud, it's not like we have to downsize everything. We still have some issues. Cloud is not going to fix those issues for us. We still have to fix it. So, if you look at it, it's still relevant. So that was because instead of understanding in-house deployment and all those administration, you now understand Cloud deployment administration as well. So, it's not black and white, that anybody can just work on anything or eliminated, it all depends there's a grey area.”</i></p>	<p>equip workers to get more jobs</p>
--	--	--	--	---------------------------------------

iii	Cloud computing will destroy more jobs than it creates in the IT workforce	Direct, inductive	<p><i>With the adoption of Cloud, there is a gradual drive towards the reduction of OPEX (people cost) which is a clear indication that the staffing model is changing</i></p> <p><i>Yes, a lot of services/applications are being automated, so need for only lesser IT staff</i></p> <p><i>firing/restructuring of service support</i></p> <p><i>Cloud is changing and will continue to change the IT security landscape; cut jobs in some cases given most organisations would have less need for on premise IT Security Engineers etc.</i></p> <p><i>h no. So the number of people is going to go down and the roles are very much going to change. The roles such as server engineer or admin is basically going to cease to exist but roles like configuration management only are becoming Tier 1 roles where they previously weren't really. Ok, so numbers down and roles are all changing.</i></p>	Cloud computing technology is enabling an increase in automation, which is may reduce existing jobs in support, data processing, and information tasks.
iv	CSPs directly influence how HEIs' teach Cloud skills	Indirect, inductive	<p><i>"Depending on the Cloud service (IaaS, PaaS, SaaS etc) and deployment (Private, Public, Hybrid etc)</i></p>	The issue of proprietorship of Cloud services makes it a difficult task for HEIs to teach Cloud skills

			<p><i>models, specific skillsets and knowledge maybe required.”</i></p> <p><i>“I don’t think we are there yet because of the competition that is going on. For example, I have a bit of problem at the moment, I am training for AWS and all that, but then automatically, if you go on to search job, you see automatically once I see something that has to do with Azure, I say no this is not for me. So, you see, already, because of the divide in the market, and I will say you see it’s not standardized. So, it makes it hard. You can only teach what is standardized, so that’s when you can bring it into the traditional system ehmm...If anyone is actually going to do a 4-year degree in Cloud, I will be like do you have to? It kind of limits and restrict you in a way from my own perspective anyway. I would rather learn the core protocols of technologies standardized in the university, then probably universities can say Ok cool. You may want to a course in AWS or Microsoft or choose from maybe. I look at the core IT skills as the cake and the proprietorship in terms of Azure Microsoft, AWS, or whatever it is as the icing.”.</i></p>	
--	--	--	--	--

			<p><i>If I'm going to give anyone advice right now, I would say, obviously, You see, that's the problem we have in IT for example, there are huge providers and it's quite hard to say do this one don't do that one. So, at the end of the day, anybody interested in that has to look at the environment, what technology is leading in that current environment. Ehmm, I wouldn't say just pick one side, I would say major in one, obviously the two big players in the market. Major in one and have the idea of the second one because It looks likes most companies like to mix and match, and not though some obviously some try to mix and match they do a little bit of Azure, they do a little bit of IBM or Amazon and all that. So, I will say major in one and learn the basics, know the rudiments. But then it's still a little bit ehm the concept of Cloud computing has to be known first before teaching any of these options.</i></p>	
--	--	--	--	--

The second hypothesis is formulated evaluating the impact of Cloud computing on job creation. The results highlight that Cloud computing would create new jobs that require new skills. Figure 5.1 shows that Cloud computing directly affects the way work is done. It brings about new functions and responsibilities that lead to the creation of new jobs and reducing the need for some specific roles. However, it is unclear from the

findings if the Cloud created more jobs than it destroyed. The third hypothesis is formulated addressing the impact of the Cloud on job destruction.

There is an overarching response from the data that the Cloud would reduce particular jobs such as administrative support roles and make some positions redundant. These roles are being automated and no longer required or reducing, but this does not mean Cloud computing is not creating new job opportunities. The second and third hypotheses are derived to examine the relationship between the amount of jobs Cloud is creating to the number of jobs that are being destroyed. Addressing this issue would help organisations planning to adopt Cloud prepare their workforce for the expected changes.

The fourth hypothesis addresses the role of the HEIs in teaching Cloud computing as undergraduate courses. As seen in Figure 5.1, Cloud introduces new business and with a lot of CSPs in the market, it is currently difficult to teach vendor-specific Cloud skills in the University. Cloud computing is not standardized and there are many vendor-specific Cloud certifications in the market. Also, the result suggests that technology is volatile, and including Cloud computing in the curriculum is not advisable. The Universities need to decide how the technical concepts of Cloud would be taught or think of the best ways to collaborate with some of the leading Cloud vendors to teach the students relevant skills that would benefit them. In terms of collaboration, the Cloud vendors have an important role to play seeing they have a more concise curriculum. Overall, the universities need a strategic plan to review the curriculum to accommodate the changing skills required. While these hypotheses are formulated from empirical data from the findings, they may be proved or disproved in subsequent research which is not covered in this study. A further quantitative study is appropriate to test these hypotheses.

5.2 RESEARCH QUESTIONS

The research questions are derived in Chapter 3. Each of the research questions is answered by using the collected data. Figure 5.2 categorizes the themes according to the research questions. Table 5.2 summarises the answers to the research questions. The evidence and answers to each question are also outlined. As can be seen from

Figure 5.2, six themes emerged in an attempt to answer the research question. These themes correspond to the answers to the research questions. The first research question is on identifying the important security skills needed to work with Cloud computing technology.

Table 5.2: Answers to Research Questions

N0	Research question	Evidence	Answer
i	What are the IT security skills required by the user organisations for the Cloud environment?	<ul style="list-style-type: none"> Section 4.3 and 5.4.1 	<ul style="list-style-type: none"> The findings in Chapter 4 attest that new skill sets, both technical and non-technical skills such as Business and analytical skills, contractual controls, innovative and critical thinking, and vendor management are needed to work in the Cloud computing environment. The research question one is answered in Section 4.3 and described in Section 5.4.1.
ii	What are the new and evolving roles for IT security professionals for supporting Cloud computing in user organisations?	<ul style="list-style-type: none"> Section 4.4 and 5.4.2 	<ul style="list-style-type: none"> The findings highlight some of the changing existing roles and new roles that the Cloud is providing. Some of the repetitive tasks and administrative

			<p>roles are being automated and migrated to the Cloud.</p> <ul style="list-style-type: none"> • Section 4.4 and 5.4.2 describes the changing roles.
iii	What are the challenges and limitations of the existing IT security skills from the organisation's perspective when confronted by Cloud computing?	<ul style="list-style-type: none"> • Section 4.5 and 5.4.2 	<ul style="list-style-type: none"> • The results highlight why the current security skills are not sufficient for working in a Cloud environment. • Cloud platforms require new skills to understand and leverage the interfaces • The limitations are discussed in Section 4.5 and 5.4.3.
iv	How should security skills be taught and what is the role of HEIs in equipping graduates with Cloud skills?	<ul style="list-style-type: none"> • Section 4.8 and 4.9 	<ul style="list-style-type: none"> • The findings suggest external professional bodies outside the Higher Education Institutes (HEI) have a more concise curriculum for teaching IT security skills. • Security should not be taught as a basic course in HEI • The best security professionals have similar disciplines and

			<p>then acquire a higher level of training in security</p> <ul style="list-style-type: none"> • The HEIs are responsible for teaching and equipping students with the basic skills needed to work in the dynamic Cloud environment. • The HEI needs to embrace Cloud technology to improve learning environments for students and provide them with the current skills that enhance their marketability in the workforce.
--	--	--	---

The research question aimed to understand the essential skills needed to cope with working in the Cloud environment. The in-depth interviews and survey data reveal that information security professionals need to have both technical and non-technical skills to cope with Cloud technology developments. The first research question is answered by the first theme which highlights 15 skills. These skills are then classified into technical and non-technical skills. Security skills are ranked as the most essential skills in the technical skills category and there is an emphasis on programming skills in the basic skills category. The implication of this is that non-technical skills are becoming essential for IT security professionals. IT security practitioners are required to adapt their skills into new environments with an emphasis on business principles and skills as opposed to only technical skills. The data does not precisely outline the exact skill sets required for successful business practice when adopting Cloud. However, the

precise skills required by an organisation to work with the Cloud are dependent on the Cloud service they are consuming, the Cloud model, the size and cost model of the organisation, and the overall Cloud strategy.

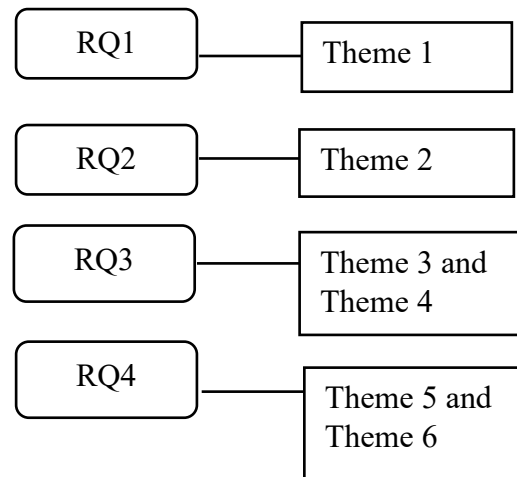


Figure 5.2: Categorization of Themes and Research Questions

The second theme answers the second research question on the changing roles. It highlights some of the traditional roles that are changing and the new roles that are being introduced by Cloud computing. Some of the changing roles include Application development, IT Support or Helpdesk roles, Network and Data Admin roles, Physical or Hardware security jobs, Security Architect, Security Engineer, Security Infrastructure Engineer, and System Admin roles. The roles Cloud is introducing include Cloud Architects, Cloud security engineer, Risk analyst, Security Architect, Security Infrastructure Engineer (Cloud-CP). It is difficult to ascertain the number of roles that are changing as this is dependent on the size of the organisation, the cost model, and the strategies used in migrating to the Cloud. However, it is clear from the result that administrative roles reduce the tasks that are automated in the Cloud. The number of Cloud roles an organisation would require largely dependent on their Cloud service they are consuming and their CSP.

The third theme answers the third research question on the limitations of traditional skills. The question aimed to understand the reason why IT security workers

think they should upskill. The limitations identified in theme three included: a need for broader knowledge, traditional skills are not so relevant in the Cloud, the type of Cloud determines the required skills, roles and responsibilities are changing and so are the required skills. The results reiterate that Cloud requires specific skills that are different from traditional skills. The capabilities of Cloud computing are reshaping the skills required to perform daily tasks. Data from the first survey reveals that all of the participants acknowledged they had to undergo training or are currently going through some training. Also, because Cloud products are proprietary, IT practitioners need to understand specific Cloud products and software platforms contrary to understanding only concepts and best practices. This might involve upskilling in different Cloud platforms as the case may be. Currently, the result shows that it is very difficult to find experts in Cloud computing and business skills that drive business innovation.

The fourth theme is on restructuring and the other impacts not relating to skills and roles. The fourth theme elaborates on the third research question on direct and indirect impacts on skills and roles. Theme four examines the overall impact of Cloud computing on the staffing model and organisation as a whole. One of the major impacts Cloud is having on businesses is changing the organisation structure. Restructuring in terms of skills, roles, work structure, security model, and management. A shift to a Cloud-native organisation would require workers to upskill, specific roles become redundant, flexible working conditions, and collaboration between the IT and other business units. More importantly, it involves hiring more competent workers that can manage Cloud services and making redundant some workers. Theme four also elaborates on cost management and the opportunity to focus on the core business. The result shows that Cloud computing increases the attack surface, and hence risk management is one of the major security skills. The data also reveals that Cloud provides the opportunity to enhance security. Some of the CSPs have made a continued investment to ensure data security, hence, they have robust security services and tools. When properly configured by the customer, the Cloud could offer a more secured environment than the on-premises settings.

The fifth theme is the role of the HEI and theme six is around teaching and learning security skills. Theme five and six answers the fifth research question on the

role of HEIs. The results show that the HEI plays a significant role in filling the security skills deficit. While the data reveals that a review of the curriculum is necessary to align with the changes in the technology landscape. Students should be taught the fundamental concepts, architecture and best practices of working in a Cloud-native environment. The data also shows that security degrees should be an advanced course taught at the post-graduate level. Security practitioners are more efficient when they had a foundational degree in computer science, software engineering, or related degree program. This aligns with the result of the University curriculum analysis. Only one of the schools has an undergraduate security program and a course on Cloud computing. This result implies that students may not be able to meet the employer's work expectations after a degree program and requires additional training or further studies. This is especially true as most employers are not ready to invest in training new graduates and would rather employ someone who has the hands-on experience to do the job.

5.3 TRIANGULATION OF RESULTS

Data triangulation is necessary to ensure the validity of the result. In this study, data is collected using primary and secondary sources. Yin (2009) proposed the concept of triangulation, in a case study to reduce bias and establish validity.

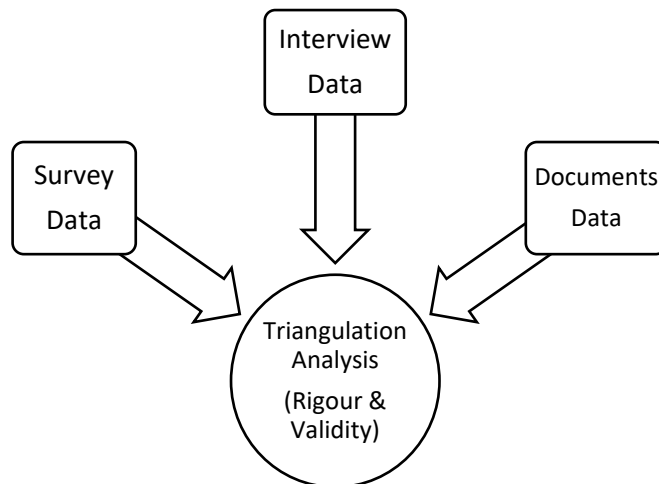


Figure 5.3: Data collection Triangulation

Yin's (2009) concept of triangulation involves using multiple perspectives to converge on the phenomenon under investigation. Figure 5.3 gives an overview of the data triangulation used in this study. The data are collected from different people at different times using different methods. Table 5.3 describes how the data sources are used to develop the themes.

Table 5.3: Triangulation Analysis

Data Source			Theme Convergence
Interview	Survey	Document Analysis	
<ul style="list-style-type: none"> ○ Scripting ○ Patching ○ Coding/programming ○ Legal and compliance understanding ○ Risk assessment and management ○ Auditing ○ Data encryption ○ Service management ○ Traffic management ○ Infrastructure Management ○ Access management ○ Vendor-specific Cloud certification such as Azure and AWS ○ Contract management 	<ul style="list-style-type: none"> ○ Basic IT skills ○ Traditional cybersecurity skills ○ Risk management ○ Data sovereignty and global privacy ○ IT management and Cybersecurity management ○ Cloud technology and architecture ○ Pen Testing, TPSAs, etc ○ Vulnerability and Patch Management ○ Security Assurance and Auditing ○ Security Administration ○ Compliance monitoring and reporting ○ Azure and AWS skills ○ Cloud Security, Security Analysis, Intrusion detection ○ Audit and governance ○ Malware analysis and reversing ○ Intrusion detection ○ Identity and access management ○ Contract management 	<ul style="list-style-type: none"> ○ Cryptographic Management ○ Information security management ○ Data and Network security ○ Secure programming and Offensive and Defensive Security ○ Digital Forensics ○ Malware and Reverse Engineering ○ Human and organisation security ○ Technology Governance and Risk Management 	<p>The data collected from each source converged. The first theme emerged as Important skills. This is then categorized as Technical (basic skills, security skills) and non-technical skills.</p>

	<ul style="list-style-type: none"> ○ Project management ○ Business skills ○ Innovative and critical thinking ○ Contractual controls 		
<ul style="list-style-type: none"> ○ System Administrators ○ Network and Database Administration ○ Infrastructure and platform support 	<ul style="list-style-type: none"> ○ Hardware support ○ System Administrators ○ Network and Database Admin ○ IT Support/Helpdesk roles ○ Security Engineer ○ Security Infrastructure Engineer ○ Application development ○ Firewall Admin 		The result converged. Each data source corroborated the findings. The second theme that emerged is changing roles.
<ul style="list-style-type: none"> ○ There is a need for additional upskilling around Cloud ○ Specific skill set is required for Cloud services. ○ I mean I think Cloud computing is changing the way we work ○ Slightly different organisational skill is required to be able to manage services in the Cloud ○ Roles are all changing ○ Requires new skills because it's a new definition of Job description ○ Issue of proprietorship 	<ul style="list-style-type: none"> ○ Requires new skills to understand and leverage the interfaces. ○ New skills are definitely required ○ Very Limited from a security point of view. ○ Different tools different skills ○ There are Cloud specific security skills that are needed ○ They are not sufficient ○ Skills not too relevant ○ The roles and responsibilities of IT professionals will change 		The results from the two data sources do not contradict themselves. The theme – Limitation of Traditional skills emerged.

<ul style="list-style-type: none"> ○ Moving into Cloud gives you an opportunity to be reactive and basically uplift your security posture ○ Cloud does contribute to security in the environment. ○ Full-time employees as that working on your core service of the business. ○ Everyone is actually forced to use a particular set of a security strategy that the Cloud provider use 	<ul style="list-style-type: none"> ○ Gradual drive towards the reduction of OPEX (people cost) ○ Saving the business a lot of money in terms of paying staff to maintain systems and servers, upgrade hardware (costly), and salaries. 		Each of the data sources gave a different perspective but do not contradict themselves. At the end of the review, the theme – other impacts emerged.
<ul style="list-style-type: none"> ○ It does reduce, obviously it takes away a lot of jobs ○ Essentially you could probably reduce staff but that's it ○ It's going to make some people idle. ○ I will say it requires some upskilling ○ Probably some downsizing of the department ○ Their function might migrate to the CSP ○ Some of the functions are eliminated 	<p>Security professionals need to train within the organisation or go to institutions that are providing the necessary training</p> <p>IT Security professionals need to keep upskilling and acquiring relevant skills.</p> <p>Cloud removes some responsibilities from the IT security professionals.</p>		The data sources outline different points that do not contradict themselves. The Restructuring theme emerged.
<ul style="list-style-type: none"> ○ I still think the institutions, in fact, I strongly 	<ul style="list-style-type: none"> ○ Understanding technology is important to be 	Incorporating Cloud courses into	Each of the data sources provides a different perspective

<p>think to believe they need to change.</p> <ul style="list-style-type: none"> ○ Need to review curriculum ○ At some point in time if possible, introduce the student ehm to the products, to the ones who are leading the market, AWS, IBM, and all that ○ Educational institution definitely needs to adjust teach more technical skills that students can actually use when they come out 	<p>effective.</p> <ul style="list-style-type: none"> ○ They need to understand the Cloud is important to be able to predict attacks/threats from a security viewpoint. ○ Roles and responsibilities exist, however additional focus on education around Cloud is required to understand the benefits 	<p>computer degree programs</p>	<p>on the question being answered. Some of the answers overlap, however, they do not contradict themselves. The theme - the role of the educational institution emerged at this stage.</p>
--	--	---------------------------------	--

5.4 DISCUSSION OF RESULTS

The following Section discusses the findings of the study according to the research question. It critically analyses the usefulness of the hypothesis, the effectiveness of the research questions, and the impact of the triangulation method.

5.4.1 Hypothesis Generation

One of the distinctive characteristics between quantitative research and qualitative research is that quantitative research uses quantifiable data to generate patterns and facts that can be used to test a hypothesis while qualitative research allows exploration of a problem for a deep insight that can be used to generate an idea or hypothesis. Qualitative studies focus largely on inductively categorizing data to generate hypotheses and theories. Hypothesis generation is one of the elements of scientific research. It proffers new ways of capturing research problems that form the basis for a new research inquiry. These are explanatory suppositions based on the data which can be tested subject to further quantitative studies. The main reason for generating the

hypothesis in this study is because there are many variables involved in the analysis and there is some level of uncertainty involved in the outcome of the result.

The hypotheses are formulated using interpretivism theory and comparative technique in thematic analysis. As discussed in Section 5.1, four hypotheses emerged from the results which are summarized in Figure 5.1. The generation began with the idea of attempting to interpreting the many variable determinants that emerged from the data into explanatory suppositions that can benefit the stakeholders of this research. During data collection and analysis, the data is compared to find the missing relationships and omissions that the questions generated. A lot of mind mapping and brainstorming took place during this stage. The aim is to establish better ways of analysing the data to answer the research questions in such a way that captures specific data that contributes to the research objectives. Using the FINER criteria, I evaluated the feasibility of the hypotheses whether it is possible to modify the existing research questions to accommodate these changes. Adding it to the research questions increases the scope of the research and cannot be reasonably studied within the time frame. It would mean seeking further ethics approval, increasing and changing the sample population, using different methods and a longer time frame. Thus, it is more efficient to have emerging questions tested in further studies.

The hypotheses are effective in explaining possible relationships that emerged from research findings that are not captured by the research questions. These include identifying contingency factors that define the skills and roles required for an organisation. As discussed in Chapter two, the CRBV and disruptive theory are applicable in hypothesis generation. Contingency theory poses that the effectiveness of an organisation is dependent on maintaining adapting activities with the subsystem and environment. The internal factors generated from the data are size, strategy, and cost model; while the environmental factors include CSP, Cloud model, and Cloud service. CRBV theory is focused on the alignment of internal resources with environmental factors to achieve optimum performance while the disruptive theory is based on the idea that existing companies who do not embrace the new technologies end up losing their business to newcomers whose businesses are built around the new and trending

technology. The following suggestions are proffered for hypothesis generation improvement:

- Clearly state the problem that you are trying to solve. This can be formed from theory, primary or secondary data
- Clearly define the variables using theory and data
- Create a list of possible explanations and ensure the hypothesis is within the scope of the research problem
- Ensure that the claims of the hypothesis are falsifiable. This can be done within the same study or through subsequent study

5.4.2 The Usefulness of the Hypothesis

The hypotheses generated from this study are useful in advancing knowledge consistent with the impact of Cloud computing on IT security skills and roles. They provide a basis for further enquiry, and define the research objectives and problem statement for subsequent research. They provide data that can illuminate the complex relationships between the complex contingencies of Cloud computing and how these variables affect the required skills and roles for an organisation.

The research questions led to many other questions. For example, the second research question is used to examine the roles that are changing in an organisation. Although this question is answered with a number of perceived roles that reduces and new roles that are been created, further details would be helpful. Some of the answers, especially from the survey respondents, could not be answered sufficiently as they simply wrote that it is not contingent on so many factors and not a one for all answer. The interview responses are clarified with follow-up questions. Overall, the many complex contingencies around Cloud computing in the data generated further questions. These questions are generated in the form of hypotheses to ascertain if the relationship between the variables exists. The formation of these hypotheses confirms the tenets of RBV theory that although IT capabilities can influence the success of Cloud deployment and help a firm to achieve a competitive advantage, the factors determining the IT capabilities are complex.

While these hypotheses do not cover all possible relationships of contingencies that determine the impact of Cloud computing on skills and roles, they efficiently

address the issues around the completeness of the research questions. The data identified cost factors, size of an organisation, CSP, Cloud model, and Cloud service as contingencies that determine the required skills and roles for an organisation intending to adopt Cloud computing. The first hypothesis, for example, addresses two of these contingencies, the relationship between the size of an organisation and Cloud service and how they determine the skills and roles. These two variables are considered as they are the most frequent variable that occurred in the data. Also, when participants are asked which Cloud environment they had worked or currently are working with, most of the respondents answered in terms of Cloud service and not the Cloud model. Furthermore, the concept of cost is relative and can mean different things to various organisations. In my opinion, the cost model is a complex variable that requires more data to properly define the concept before speculating possible relationships. Similarly, in an attempt to answer the second and third research question, the result shows that the roles that would be migrated to the Cloud, reduced, or become redundant are determined by the size of an organisation, CSP, Cloud model, and Cloud service. Based on the results of the study and CRBV theory, the following recommendations of possible relationships are drawn for future study:

- The contingencies that determine the skills and roles required are the same for a small, medium, and large organisation
- The type of Cloud service determines the skills and roles required for the Cloud model
- CSPs are the main determining factor of skills and roles requirements, and not the Cloud service nor Cloud model
- Universities that work with CSPs will produce more competent graduates
- Cloud proprietorship and lack of standardization will hinder its adoption into the teaching curriculum.

5.4.3 Research Question Contribution

The research questions formulated in this study are useful in defining the scope of the research interest. They focus on the purpose of the research and serves as a guide for the research design and overall process of conducting research. Ultimately, the research

objective is to enquire into IT security personnel's perception of the impact of Cloud computing on IT security skills and roles. Surely, this is of interest to the education policymakers, educators teaching information security/ cybersecurity, and to businesses in the industry intending to adopt Cloud computing. Therefore, the research questions are designed to answer questions that would be beneficial to these stakeholders.

As discussed in Chapter 3, the research question is formulated using the FINER technique. The research questions are formulated from secondary data. The qualitative approach and interpretivism paradigm shaped the way the research questions were asked. From Chapter one and two, the research problem and research gap are identified. It identifies that people's jobs are being commoditized, outsourced, and paid for as per use in the Cloud. This is leading to redundancy and job loss of people who do not have Cloud competencies.

The research questions are effective in exploring the overall impacts of Cloud on IT security skills and roles in an organisation. It identified 15 skills required to work in a Cloud computing environment. It also identified specific roles that are becoming redundant and the new roles that the Cloud is creating. Most importantly, it validates that the Cloud is changing how people work and IT security practitioners need to adapt their skills to the new work environment. These results align with the tenets of contingency theory as discussed in Chapter two. When adopting Cloud computing, workers should understand that security skills and roles also need to adapt to the new environment effectively. Furthermore, Universities play a major role in preparing students for the new work environment, and skills validation through professional certificates is becoming an essential requirement for employers. These two bodies play a necessary role in bridging the security gaps in the cybersecurity workforce. This result agrees with RBV theory that having a skilled workforce with IT capabilities can influence the success of Cloud deployment and help businesses achieve a competitive advantage.

During data analysis, there are times I felt discontented with the lack of analysis. This is observed during data collection. Rather, several other complex factors need to be considered before answering the research questions. There are a number of

additional questions that need to be considered. Although as I reflected on my notes, got deeper into the analysis and combined the data from different methods I am able to answer the research questions. Research questions one to four are dependent on many factors. This result also aligns with the CRBV theory discussed in Chapter two. Cloud competencies require constant adaptation and change which could be related to the maturity levels of Cloud implementation in an organisation. Maturity depends on the skills and how the staff implements the Cloud. Thus, the research questions seem too broad to capture how Cloud computing impacts different organisations according to their size. Also, considering the competition in the Cloud market, the questions could benefit from a more focused study that captures the specifics by comparing two Cloud services such as SaaS and one or two CSPs. From the data, SaaS is the most consumed Cloud service and AWS and Microsoft Azure are the most used CSP. Furthermore, revising the research method to include both quantitative and qualitative approaches would yield more compelling results.

Considering this study is guided by the qualitative approach and CBRV theory, the following recommendations are made for future study:

- What are the contingency variables that determine roles and skills required when using PaaS, SaaS and IaaS in Microsoft Azure and AWS
- What are the skills and role requirements when using PaaS, SaaS and IaaS
- How does Cloud computing impact small, medium, and large organisations in terms of required skills and roles?
- What roles are made redundant when using PaaS, SaaS and IaaS
- What is the percentage of new roles does Cloud create for small, medium, and large organisations.

5.4.4 Implications from Triangulation Strategy

The purpose of the triangulation is to ensure validity and provide completeness of data from different perspectives. It is one of the ways of establishing validity in qualitative research (Meijer, Verloop, & Beijaard, 2002, p. 146). Glinner (1994) argued that the purpose of triangulation is to have different patterns of agreement based on more than one method, observer, or data source (Glinner, 1994, p. 84). The triangulation in this

study involves a systematic combination of different data collection methods (interview, survey, and document analysis) to establish different interpretations and verify the findings. These methods provided a different perspective on the data which is comprehensive and rich for making meaningful deductions. The aim of the triangulation for this study is not to establish agreement from different methods rather for completeness; to combine the data from each method and have a comprehensive view of the impact of Cloud computing on IT security skills and roles.

The procedure for the triangulation gradually emerged from the literature review which is based on the interpretivism/constructivism theory. This is based on the tenets that there are multiple realities and knowledge is gained interactively. It is assumed that having multiple data sources through different methods provides a comprehensive perspective on the research problem. For this research, I am the sole investigator who interacted with all the participants. While constructing knowledge from the multiple realities from the participants, I made sure my assumptions are not impacted in the research process and interpretations. I approached the research with the understanding that Cloud computing is causing disruption and disintermediation is bringing severe shifts in an established business. While I had my preconceptions about the study, I am careful not to project or reflect my own bias. To achieve this without compromising my ethical responsibilities as a researcher, I kept research notes that included my reflections during the data collection and analysis stages. It is important to note my possible assumptions of data analysis so as not to project my bias onto the data interpretations. The data are categorized and compared and conclusions are drawn.

The methods that are used for the triangulation are effective as they complement each other. Each of the methods complements the other and increases the in-depth understanding of the research problem. The interview provides rich data that could not be achieved with surveys and documents. The secondary data from the documents is used to capture how the universities are preparing the students for the workforce. It compares the skills being taught with professional certifications skills. The survey is useful in providing an understanding of opinions, measuring attitudes, or an individual's reflection of reality on the skills and roles required for a Cloud computing environment. Also, considering one of the inherent limitations of qualitative case study

methodology is the lack of rigour, the use of multiple data collection techniques increases the rigour and validity. The combination of the methods in itself has no limitation in producing the desired result as this depends upon the design. Overall, the hypotheses generation benefited from the triangulation strategy.

The triangulation strategy clearly provided diverse data that helped in answering research questions especially with research question five. The data from the documents provided insights into what students are learning in relation to what is expected of them. Though the documents increased the overall perspective of the data, it is not comprehensive enough for answering other research questions. The design is not efficient for achieving the research objectives. A more comprehensive document data collection could include collecting data from job advertisement sites to examine IT security job descriptions before and after Cloud computing technology. The job description could span 10 years for jobs before Cloud and five years after Cloud. Also, the survey data did not provide enough data on research question five.

In conclusion, researchers should approach method triangulation with caution. The triangulation approach could lead to the inconclusiveness of data if methods are incompatible. Based on personal reflection of the overall triangulation process and the findings of this study, the following are recommended for future studies:

- Choose the triangulation type during the research design.
- Clearly state the role of the researcher and how bias is overcome.
- Choose methods that can gather the required data for the research.
- Ensure the chosen methods complement each other.
- Ensure that each of the methods used addresses all research questions.
- Extend triangulation to include both quantitative and qualitative approaches.

5.4.5 Result Implications

This section discusses the results that have been presented in Chapter four. It relates the results to existing literature. It highlights the implications for various stakeholders including students, IT security professionals in the industry and academia.

5.4.5.1 Important Skills

Cloud is changing the focus of IT practitioners and the future skills requirement. The first theme that emerged is the crucial skills required by the user organisation. In making a change to deploy Cloud computing in an organisation, the roles and responsibilities also shift, requiring a new set of skills. Sousa and Rocha (2019) identified Cloud Technology, Internet of Things, Big Data, Mobile Technologies, and Artificial Intelligence and Robotics as significant technology advancements disrupting business models and requiring specific skills and competencies.

The implication of the study is that information security professionals need to have both technical and non-technical skills to cope with Cloud technology developments. While security skills are essential skills in the technical category, the basic skills are still necessary and fundamental in working in a Cloud environment with an emphasis on programming. Cloud is driving automation, and programmability is a crucial concept in the Cloud evolution. Security skills and service-related skills are ranked as the core of the skills required in the Cloud (Laugesen et al., 2012, p. 72). Security skills are considered to be an essential skill required for IT professionals. There is a growing demand for business, management, and security skills (Laugesen et al., 2012, p. 8). This is because the Cloud presents new and higher security threats and challenges. The result also shows that basic skills are still important and fundamental in working in a Cloud environment. There is an emphasis on programming skills in this category.

While professionals are expected to be competent in technical skills to work with Cloud technology, non-technical skills are now being required for employment. These include critical thinking, production and management, people management, emotional intelligence, judgment, knowledge negotiation, and cognitive flexibility (Xing & Marwala, 2017, p. 10). The result reveals that non-technical skills such as project management, critical and innovative thinking, vendor management are considered crucial when working with Cloud technology. These results align with the literature. For example, Ross (2011) confirms that there is a focus on soft and or intangible skills such as communication and interpersonal skills, project management, contractual controls, and management (Ross, 2011, p. 69). Also, regarding innovative and critical

thinking, Leopold et al. (2018, p. 7) reveal that organisations would need a new strategy to reimagine the routines and limits to successfully maximize Cloud technology to achieve a competitive advantage. Similarly, Sousa and Rocha (2019, p. 260) highlight innovative and creative skills as one of the main skills needed by business managers affected by disruptive technology such as the Cloud.

5.4.5.2 Changing Roles

Cloud computing is changing the landscape of jobs, and traditional roles are rapidly changing. It has simplified IT operations that many roles in IT are becoming unnecessary. In a traditional environment, skills and roles are well defined. Traditionally, business leaders specify functional specifications that are assigned to the IT team to identify the best technical approach. The IT then meets this requirement using the existing technology and IT resources within the company. However, sometimes this may require some form of outsourcing or investment in new technology or skills. Cloud is changing this process and introducing new skill requirements and allowing the business management to exert much greater control over IT/business solutions (TCBC, 2016, p. 2). The result reveals that Cloud technology is driving automation, which is changing the way IT services are consumed and deployed. It drives business growth and allows the IT team and leadership to focus on strategies and achieving business goals efficiently. However, it also poses the risk of displacing roles when specific work tasks become obsolete or automated (Leopold, Ratcheva, & Zahidi, 2018, p. 6). The Cloud is simplifying IT operations that many roles in IT are becoming unnecessary (Anderson & Gantz, 2012). The traditional role of IT in an organisation includes the maintenance of corporate infrastructure, updating systems, as well as providing support, which is changing. The IT department recruits IT professionals, such as systems administrators, developers, and IT support technicians, to perform these tasks.

However, this is changing as Cloud is causing a decline in some roles, especially in design and architecture, development and deployment, and user support (Laugesen et al., 2012, p. 75). As businesses consume Cloud services, the need for specific designing of systems from scratch is reducing as organisations now purchase Cloud existing solutions and adapt them to meet their needs. Also, there is a reduced demand

for support administrators as platforms and infrastructures are now outsourced to Cloud providers who provide the needed support. Also, Ross (2011) believe that user-support people in general roles in organisations that are not IT-focused would be more prone to redundancy than the specialized ICT workers in the Cloud environment (Ross, 2011, p. 68).

The result also suggests new roles are created such as the Cloud architect which is crucial for successful Cloud migration. According to Gartner, Cloud architects have three main tasks: leading cultural change for Cloud adoption, developing and coordinating Cloud architecture, and developing a Cloud strategy, and coordinating the adoption process (Hilgendorf, 2016, p. 4). Though some roles remain the same, their daily responsibilities have significantly evolved. For example, roles such as application development have evolved into DevOps and DevSecOps. While some organisations may still refer to this role as an application developer, most organisations now refer to them as DevOps. Irrespective of the role name, their responsibilities and capabilities have changed. Application developers in the Cloud no longer use the traditional waterfall model; they now employ new methodologies. DevOps methodology combines software development and IT operations concurrently while DevSecOps extends security practices into DevOps. The goal of this new methodology is the use of automated delivery pipelines to reduce the software delivery cycle time. Overall, according to Carraway (2015), the most notable changes to the industry are the impacts on IT staff roles. For IT staff to be able to function and support Cloud technologies, they need three things: An understanding of their roles and any changes to their current position, time and resources to explore the technologies, and an understanding of the business case for the technologies (Carraway, 2015, p. 4)

5.4.5.3 Limitation of Traditional Skills

Cloud technology, like many other emerging technologies, is changing every aspect of work. These transformations have led to widening the IT skills gap in the IT industry. Leopold et al. (2018) observe that technology transformations could lead to increased skills gaps among workers and leadership, greater inequality, and broader polarization when not adequately managed. With the rise in automation, technology may free up existing jobs in support, data processing, and information tasks (Leopold et al., 2018,

p. 3). Business owners fear that their existing staff may not be able to manage the Cloud effectively when they move to the Cloud (Laugesen et al., 2012, p. 96). The implication of this is that IT workers need to upskill to remain relevant or be made redundant because more employers are seeking employees with new skills. The traditional skills do not align with evolving task demands in the Cloud environment.

Furthermore, the findings of the study affirm that apart from having to adapt to the new working environment and changing responsibilities, they are also required to learn some non-technical skills which have become important for their new role. The focus has always been on technical skills, but soft skills have become crucial in the information security workforce. People's skills must align with the required tasks to meet the organisation's needs. The findings are consistent with the research literature (Ross, 2011).

5.4.5.4 Other Impacts

Another impact of Cloud computing from the findings of the study is the requirement for organisational restructuring. Cloud technology, like any of these emerging technologies, are changing the nature of jobs, destroying jobs, and creating new jobs. There is an unprecedented job loss because of the steep learning curve for Cloud technology (Nübler, 2016, p. 1). It would displace some workers as businesses seek to hire qualified, and skilled workers. The findings of this study also reveal that information security workers need to upskill and there is more emphasis on certifications. This agrees with the CSIC study, which indicates that companies prefer people with certifications and hands-on experience from training, rather than having only a bachelor's degree. Cloud is introducing new skills, which means practitioners being able to learn new skills to get prepared for the redefined roles (Ross, 2011, p. 69). The overall implication of Cloud for jobs is that workers who are skilled in adapting to the Cloud technology environment are in high demand while workers lacking appropriate skills may find themselves redundant or out of a job. Not having skilled workers would broaden the existing skills gap in the cybersecurity workforce. Cloud leads to firing, hiring of new staff, reduced staffing in some cases, and roles migration and adaptation.

Furthermore, the study also identified other impacts the Cloud is having on the

organisation. Generally, Cloud computing technology has caused some form of disruption to the business model of an organisation. Leopold et al. (2018) identified Cloud technology, ubiquitous high-speed mobile internet; artificial intelligence; and widespread adoption of big data analytics as to the four significant technological advancements to business models and practices (Leopold et al., 2018, p. 6). The study reveals that the Cloud is generally providing opportunities to enhance security. The Cloud security model for an organisation is dependent on its strategy, contractual controls, and CSP.

Also, the study acknowledges that the Cloud could save costs, especially in terms of infrastructure, and provide opportunities to enhance security. Cloud saves the cost of purchasing infrastructure and maintaining the IT systems. It offers an on-demand service that provides an opportunity to scale up or down. Most of the participants believe that using Cloud services in your organisation does not necessarily increase security and can expose the business to more threats. However, depending on the business strategy, SLA's, and contractual agreements, the Cloud may improve security. Cloud could provide a more secure environment compared to the on-premise servers. Cloud is as secure and cost-effective as the business plan and strategy. It is because Cloud providers use a shared security model to address Cloud security risks. Every organisation needs to understand its responsibility in ensuring security in the Cloud. The Cloud providers are usually responsible for securing the system, infrastructure, and platform while the individual organisation is responsible for securing their data. Additionally, because of the reduced infrastructure administration, using the Cloud helps business leaders and IT teams to focus more on strategies to align business. The resources are focused on utilising Cloud services on business strategy and innovation to achieve a competitive advantage.

5.4.5.5 Learning and Teaching Security Skills – Role of HEIs

Two important themes that emerged while answering research question five are how and where security skills should be taught and the role of HEIs in teaching these skills. Some of the participants reveal that teaching security as an advanced course in a postgraduate program is more beneficial than having it as an undergraduate course. It is argued that some of the best security experts are from diverse backgrounds in other

degrees such as computer science, engineering, law, or even social sciences before majoring in security. They have an understanding of the theory and fundamentals from their degree program or have gained hands-on experience in the profession. There is also an emphasis on certifications as most degree programs do not usually meet the employer's skills requirement. A recent report predicts that there would be 3.5 million unfilled cybersecurity positions by 2021 (Morgan, 2017).

Furthermore, the findings implied that learning security skills in an informal environment rather than a traditional school setting is more efficient for an immediate solution to bridging the cybersecurity skills gap. Lurie (2017) proposed that one of the ways to fill the skills gap is to focus on employee's skills and not on the degree. The study suggests looking into professionals who may not have a traditional college degree but do have the required technical skills needed for the job. Similarly, a report by Crumpler and Lewis (2019) reveals that apprenticeship programs have more hands-on and practical experience than most cybersecurity graduates (Crumpler & Lewis, 2019, p. 4). A degree is usually not sufficient, and additional training certifications for practical learning opportunities are crucial in working in the rapid and dynamic security environment. Also, employers seem to view candidates with certifications as more qualified than degree holders. There is a gradual decline in the value of degree programs for cybersecurity jobs (Crumpler & Lewis, 2019). Professional certifications and hands-on experience are ranked as a better way to achieve cybersecurity skills rather than a degree program as academic institutions are struggling to change the curriculum to align with the pace of the industry.

Another key finding of this research is the role of HEIs. Schools, colleges, and universities play an integral part in a functioning society (Anderson, 2010, p. 4). The HEI is crucial in every modern society ready to embrace change. Cloud technology creates different challenges and opportunities for students in the learning environment (Xing & Marwala, 2017, p. 10). IT is a rapid, dynamic, and volatile industry. In speciality fields such as IT, it is impossible to be experts in all technology products, and individuals have to decide which technology to learn. One of the participants, P18 recommends the formalization of institutions that can teach cybersecurity skills that make a career path for students—*"I hope they really do start having probably non-*

degree but technical certification. I mean, so, like you are a Cloud security engineer, but not necessarily a degree, but you must have gone through, for example, AWS and Azure. Maybe the formalization of that intuition. It will be like institutions and starts offering that as this is a course where you come, you learn for a year. As a result, you can go into working in either AWS and one of the data center or for software as a service business or but not necessarily both”.

Furthermore, the study shows that the issue of proprietorship is a challenge to acquiring Cloud skills. The training and courses offered by the Cloud vendor community are specific to their products and services. Having this in mind, the implication of this for a HEI is the difficulty in teaching what is not standardized. There is a need for a universal baseline standard for security skills. Reviewing the curriculum to teach technology-relevant skills to prepare students for the workforce is a time-based challenge.

The industry vendors tend to be up to date in modifying their training and curriculum to satisfy the market requirement. Educational institutions, however, have been criticized because they are slow to adapting and adjusting their programmes to include skills to meet the ever-changing demands of industry (Laugesen et al., 2012, p. 96). A study by the Center for Strategic and International Studies (CSIC) indicates that only 7 percent of schools do a major or minor in cybersecurity programs and 33 percent at the Master’s level. The study also shows that 23 percent of Universities are providing students with the required skills for the cybersecurity workforce (CSIS, 2016, p. 10). While reviewing the curriculum might be a lengthy process for the HEI, they need to keep up with these changes in the market by aligning their programmes to meet the industry skills required because employers are not keen to hire the workers they would train. They are seeking candidates with specific skills for the job.

Students require new skills to be well prepared for the changing global workforce environment. This may mean revisiting educational and curriculum policies to accommodate the changes Cloud is bringing to the academic environment. Students need to be guided in ways that enable them to produce knowledge rather than just receiving information. Creativity and innovative thinking are critical to the new learning environment. Educational institutions should provide enabling environments

to facilitate teaching, learning, research, and development activities that align with the changes and advancement in technology (Silverstone, Phadungtin, & Buchanan, 2009). The teachers need to understand how to use technology to facilitate meaningful learning that enables students to construct deep and connected knowledge applicable to real situations (Ertmer & Ottenbreit-Leftwich, 2010, p. 257).

While technology advancement, such as Cloud computing, continues to impact the educational institution, the goal remains unchanged. The purpose of higher education is to provide quality learning through teaching, to provide students with the latest knowledge through exploratory research, and to sustain the development of societies through service (Xing & Marwala, 2017, p. 12). Therefore, as the HEI embraces Cloud technology to improve learning environments for students through eLearning and digital learning, students must be prepared with the current skills that enhance their marketability in the workforce.

5.4.7 Modified Framework

Organisations face conditions that are frequently changing and require leaders and managers to reevaluate problem and solution activities (Nadler & Tushman, 1980, p. 47). Technology shifts are a significant driver of these changes. Regardless of how organisations view Cloud computing, Cloud computing is causing a significant change in the required IT security skills and roles in user organisations deploying Cloud. As the IT environment changes with Cloud technology, it is essential to identify and evaluate these changes.

Figure 5.4 provides a modified conceptual framework (compare with Figure 2.2). The modified framework suggests that adopting Cloud can be disruptive. However, having the right strategy and aligning the organisational processes with competent staff improves the organisations' effectiveness. The modified framework highlights the external Cloud factors as regulations in terms of data sovereignty, Cloud models, CSPs, and Cloud services. While the internal factors are work, process, and people. The Cloud business environment is affecting the people, the processes, and how the work is done in an organisation. There is a redefinition of the existing skills set and the creation of new skills because of the Cloud external environment. People are required to have both

soft skills and technical skills. Also, the demand for some traditional IT roles are reduced and new roles are also been created.

These changes are a result of the external Cloud contingencies such as Cloud service, Cloud models, and competitors from CSPs. The alignment of these external factors with the people, processes, and work is crucial in achieving the organisation's effectiveness. Furthermore, the findings suggest that the manager or business leader needs a deep understanding of the organisation's processes and an inclusive leadership style to drive the necessary change. It also includes understanding an individual's motivation for change that can drive or hinder change. The results also add that HEIs are responsible for bridging the skills gap by equipping the students with the relevant skills needed for the workforce. A number of conclusions can be drawn from the findings presented in Chapter four that relates to the research questions. Although the sample population for gathering the data is small, the result is still able to provide meaningful insights into best practices for organisations planning to migrate to Cloud computing in terms of skills and role requirements. There is a need for constant evaluation of the organisation structure, and skilled and competent people to ensure they are consistent with the evolving work demands in the Cloud.

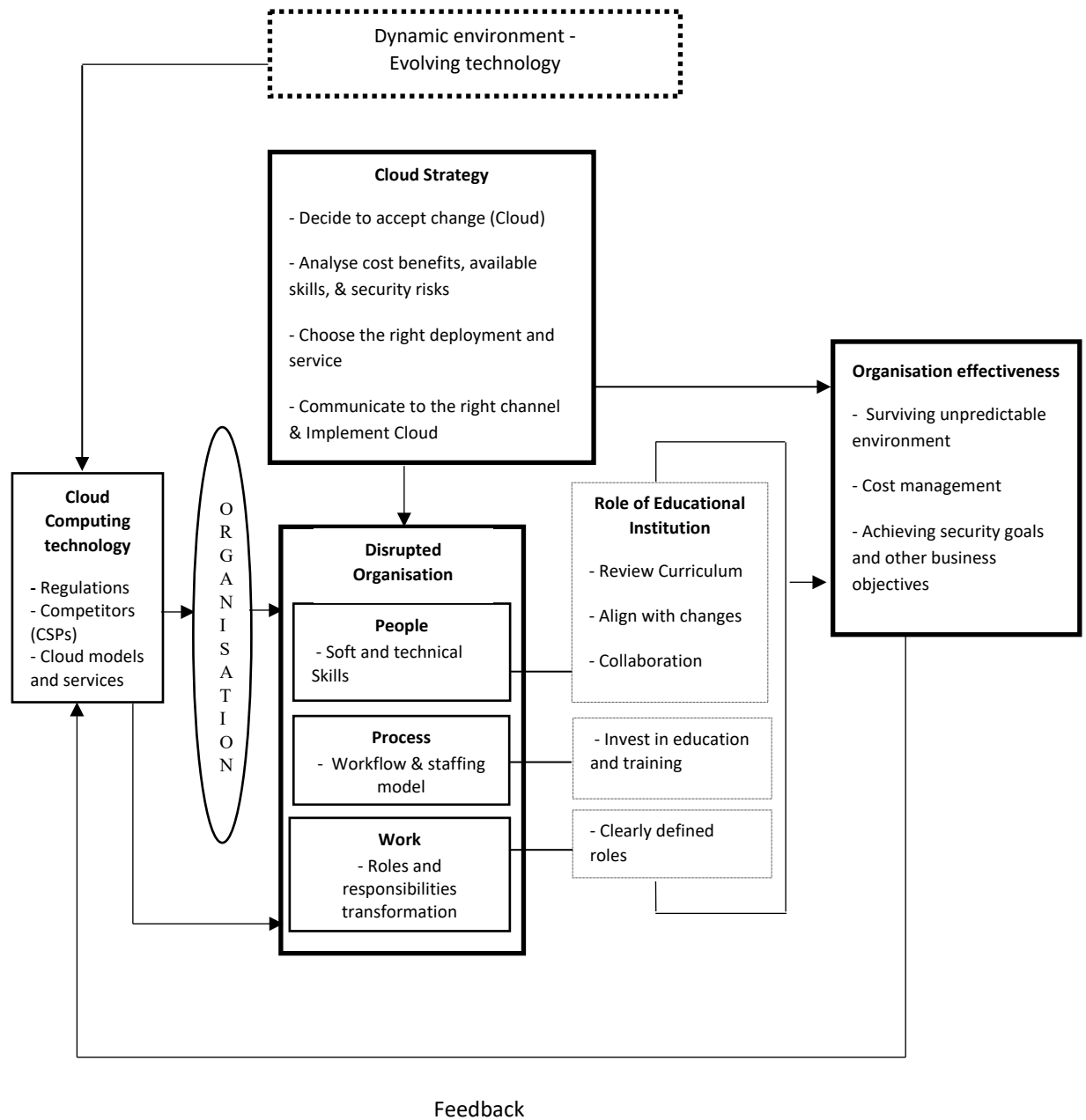


Figure 5.4: Revised Framework

These changes are a result of the external Cloud contingencies such as Cloud service, Cloud models, and competitors from CSPs. The alignment of these external factors with the people, processes, and work is crucial in achieving the organisation's effectiveness. Furthermore, the findings suggest that the manager or business leader needs a deep understanding of the organisation's processes and an inclusive leadership style to drive the necessary change. It also includes understanding an individual's

motivation for change that can drive or hinder change. The results also add that HEIs are responsible for bridging the skills gap by equipping the students with the relevant skills needed for the workforce. A number of conclusions can be drawn from the findings presented in Chapter four that relates to the research questions. Although the sample population for gathering the data is small, the result is still able to provide meaningful insights into best practices for organisations planning to migrate to Cloud computing in terms of skills and role requirements. There is a need for constant evaluation of the organisation structure, and skilled and competent people to ensure they are consistent with the evolving work demands in the Cloud.

5.5 CONCLUSION

This study aimed to identify the impacts of Cloud computing on IT security skills and roles. The research process involved qualitative data collection using interviews and online questionnaires. A thorough thematic analysis is performed on the data. The study highlights significant impacts of cloud as demand for new skills, both technical and non-technical skills, roles restructuring and redundancy, firing and hiring of professionals, and the right advanced skills. The findings also indicate that Cloud adoption leads to greater skills gaps, which causes a high rate of job loss. Participants affirm a way of adjusting to these changes is to align the Cloud strategy with competent, skilled IT professionals in order to maintain a skilled cybersecurity workforce. The HEIs need to provide the students with core skills to meet the demands of the industry.

The study clearly outlines the impact of the Cloud on skills and jobs. It provides the practical implications of Cloud computing to the organisation and academia. Alignment of the strategy to the environment, competent professionals that organisation leaders and managers can fully utilise, and optimised design can realize the benefits of Cloud technology and competitive advantage. Chapter six provides the research summary, the limitation of the study, and future work.

Chapter SIX

Conclusion

6.0 INTRODUCTION

The primary purpose of this study is to understand better how Cloud computing has impacted the type of skills and job roles required by IT security professionals who have adopted Cloud in their organisations. The study has highlighted these impacts through literature and primary data collected. It also discusses the contributions and challenges.

Chapter six summarises the overall research findings and highlights the contributions. Section 6.1 summarises the findings of the study. Section 6.2 provides the limitations of the study. It discusses how the characteristics of the research methodology impacted the findings. Section 6.3 highlights the recommendations from the exploratory findings for quality improvement and further research. It outlines the significance and benefits of the study and discusses how future research can extend the project to provide further perspectives on the impacts of Cloud technology adoption on IT security skills and job roles. Section 6.4 suggests future work for further research.

6.1 SUMMARY

This research contributes to the body of knowledge by answering three main research questions. The first question is concerned with identifying the crucial skills needed by professionals to cope in a Cloud environment. The second question investigates the changes that the Cloud is bringing to IT security job roles, and the third question is concerned about the new and evolving roles and knowledge required for IT security professionals for supporting Cloud computing in user organisations. To inform the study, Chapter two reviewed relevant literature on the evolution of system architecture and information security as well as the current issues of adopting Cloud computing in an organisation. It provided insights into researchable problems and facilitated identifying research gaps, which provided knowledge that led to research question formulation for the study. It also discusses suitable open system organisation theory to expedite understanding and interpreting organisational changes. Furthermore, it

presents a conceptual framework to explain the main components to be studied as well as the relationships between the components.

Furthermore, Chapter three captured relevant methodologies to achieve the aim of this study. It also presents a review of similar methods from the literature and philosophical underpinnings. It provided knowledge useful for the systematic selection of the chosen research method. An interpretative qualitative case study methodology is selected as the most appropriate for this study. The data is collected using interviews and online surveys, and the data is analysed using the thematic analysis framework. The prospective participants and respondents are sent invitations. Upon acceptance, the participants sign and return the ethics form. It also discusses the research design and its limitations.

Chapter four presents the results of the study. The study uses NVIVO data analysis software to carefully analyse interview and survey data. The use of NVIVO increases the efficiency and effectiveness of interpreting data. The study adopts Yin's (2009) case study analysis and thematic analysis process. The stages included familiarization with the data, initial coding, categorizing and identifying themes, reviewing themes, defining and naming themes, and presenting the results. Overall, six themes emerged from the findings: the important skills, the evolving roles, restructuring (limitations of the traditional skills, upskilling), other impacts, the role of HEIs, and learning information security, as can be seen in Table 4.4. Each of these themes is elaborated and supported with quotes from the interview and survey excerpts.

Chapter five discussed the findings and justifications from the literature. The results show that there is a need for constant evaluation of the organisation structure and people's skills to ensure they are consistent with the evolving work demands in the Cloud. A modified framework of the conceptual framework presented in Chapter two is presented in Figure 5.1. It also highlights and discusses the implications of the study for academia and the organisations intending to adopt Cloud. Furthermore, four hypotheses are generated from the results and it answers the research questions. Overall, the result of the study offers some insights into the required skills to cope in the Cloud. First, it highlights that Cloud computing significantly affect staffing. The findings suggest that using Cloud services does not eliminate IT security roles. Instead,

it reconfigures the roles. While user organisations might experience a decline in some roles, the CSPs need to hire new staff to work with them. The changes may result in making some roles redundant, thereby leading to firing and possibly hiring for new roles or training of existing staff. It may pose a significant challenge to IT professionals that now require new skills. Secondly, the study highlights that the skills needed to work in a Cloud role differs significantly from traditional IT roles. IT security professionals now require both technical and non-technical skills to work in the Cloud. Soft skills are becoming essential, which are initially not required.

Thirdly, the findings outline the role of the HEI in bridging the Cloud skills gap. The results acknowledged that graduates are not provided with the skills they need to cope in the workforce, and the higher institutions need to review and revise their curriculum to update the changes and advancements in technology. The results also highlight that security is an advanced and specialist field that requires hands-on experience, and sometimes needs further training or education. Ensuring the cybersecurity curriculum meets the potential requirement of the cybersecurity workforce is essential in meeting the skills gap. The findings recommend collaboration between the vendor community, Universities, and professional organisations. The vendor community and professional organisations can contribute to University requirements understanding. The Vendors can also provide access to their Cloud products at affordable rates so students can experience and learn the systems. Most Universities offer generic computer science with some specialist modules or courses in security but need to also teach non-technical skills, which are also essential to cope in the dynamic Cloud environment.

Finally, the last Chapter, Chapter six, presents a summary that highlights the key contributions and recommendations for future studies. It provides a framework that defines the skills required to work with Cloud computing technology. It also outlines roles transformation from a traditional work environment to a Cloud environment. This framework provides the background for making informed and appropriate decisions about the workforce when adopting Cloud computing. It also advises a review of the academic curriculum to include training solutions that provide relevant IT security skills. Overall, it adds to the body of knowledge by providing expert opinions on the

skills perceived necessary for the IT security professional workforce in Cloud computing.

6.2 LIMITATIONS OF STUDY

The study shows several impacts the Cloud is having on the required skills and roles for IT security. As with any study, the limitation of this study is inherent in its research method. The result of this study is based on qualitative data, which can be biased or judgemental. The conclusions drawn are based on the expert's opinion and are not irrefutable facts. Also, the data collection and analysis process is subjective and dependent on the researcher's interpretation.

One of the main limitations of a qualitative study is the generalisation of the results. The generalizability of this study is limited to its sampling method and population. Also, a purposive sampling method is used to collect data. Therefore, the result is non-representative and cannot be accurately generalised for another population. However, the purpose of the case study is to explore an in-depth investigation of individuals and groups with respect to the impacts of Cloud computing technology on IT security professionals in terms of the required skills and changing job roles. The data obtained from the sample is adequate to provide detailed descriptions that answered the research questions and to provide starting points for further research.

6.3 RECOMMENDATIONS

The result of this study is useful to academia, which plays a vital role in filling the current skills gap in the cybersecurity workforce. It is also useful to the industry for planning and preparation for the workforce when adopting Cloud computing. The results highlight the skills required for Cloud technology and experts' opinions on how higher education can help in filling the skills gap. A clear understanding of the required IT security skills and roles facilitates the changes that must be made to current roles and knowledge requirements. It is essential to design appropriate information security education programs to meet the needs of the industry. The findings also suggest some factors to consider for organisations in the process of adopting Cloud technology. This Section highlights some recommendations for industry and higher education institutions for teaching Cloud security skills.

6.3.1 Cloud Security Education

One of the key suggestions in the findings for higher institutions is having an industry-aligned curriculum by collaborating with the industries and Cloud Vendors. Most of the Cloud-based skills required by Information security professionals are industry-based. Cloud is not standardized and not easy to teach. Also, higher institutions are not designed to rapidly change the curriculum. However, with the reality of the impact of Cloud computing technology, equipping students with Cloud skills is essential. While the result shows that technology is volatile and schools should make sure they are not driven by big technology players in the industry. It is essential to teach relevant skills that capture the current technology in IT to students to enhance their value to the workforce. One of the ways to achieve this is by having an industry-aligned curriculum. AWS recently launched its AWS educate initiative that teaches Cloud skills to students between the ages of 14 to 17. It is also partnering with some colleges and universities in the USA to develop Cloud training programs (Kroonenburg, 2020). The idea is to promote its Cloud platform as well as attempt to bridge the current skills gap. This initiative is expected to capture future employees and possibly create a career path for students.

Another example is the Cisco networking certificate which is recognized globally. Some schools undertake degree programs that prepare students for the Cisco CCNA certification and the requirements of CCNP certification. Though the knowledge is limited to Cisco products, the course meets the market demands and creates a career path for graduates with cisco. Universities should consider doing something similar for the Cloud and start offering Cloud skills courses while not forfeiting the purpose of formal education. They can leverage organisations and professional bodies to build Cloud skills and capabilities. Having a balanced industry-aligned curriculum and investing in Cloud education to build a foundation of success for students in the workforce.

6.3.2 Organisations Adopting Cloud

The study also acknowledges some elements that should be considered by business owners or organisations thinking of adopting Cloud or in the process of adopting Cloud

technology. One important element is Cloud strategy. This includes accepting the need for change, analysing cost benefits, the available skills, security risks, and choosing the right deployment and service. Accepting the need for change is the first step to benefitting from the Cloud. Cloud computing technology has experienced rapid growth over the past decade and it is changing the existing business model. Business owners and leaders need to understand and embrace these changes. These can be in terms of IT processes, possibilities of advanced security, automation of processes, unlimited storage, reduced operating costs, and an overall change in the structure. Strategies such as involving the staff in the plans for a change can make the transitioning easier.

Another key factor from the result is in understanding the cost benefits of adopting Cloud especially in terms of skills, roles, and security implications. The findings suggest that the size of an organisation, as well as its requirements, determines whether an organisation adopts the Cloud. Cloud computing introduces new skills and roles. An organisation needs to consider the required skills, existing skills, and missing skills before adopting Cloud. Also, what is the cost of hiring competent staff to manage the Cloud or the cost of training existing staff? Are the current staff willing to upskill? How much is the organisation willing to invest in training and education. What plan is in place for workers whose roles might become redundant? These are some of the deliberations that need answers. Furthermore, the issue of data sovereignty and privacy needs to be considered. Also, risk management and compliance are some of the major issues of adopting Cloud. An organisation needs to consider the security implications, such as can your data be stored across different nations, or do you still need some on-site storage, can you guarantee your data is secured? Auditing and SLAs agreement are factors that should be considered. Although there may be several benefits of using Cloud technology, it might not have sufficient cost-savings in some organisations. The importance of having a cost analysis is to understand the value of a change. The overall goal is to ensure a smooth process of adoption and to gain a competitive advantage over other competitors.

6.4 FUTURE WORK

The purpose of this study is to understand how Cloud computing is affecting the IT security skills and job roles of IT professionals who have adopted Cloud in their organisations. A clear understanding of the impact of Cloud computing on skills and roles provides the opportunity for more effective management of organisations by planning to use Cloud services. One of the identified limitations of this study is the sample size. A recommendation for further studies will be the research population. Having a wider population sample size with participants from more industries provides a comprehensive perspective on the overall impact of Cloud computing on IT security skills and roles.

Based on the findings, it is impossible to quantify the impact Cloud is having on IT security skills and roles, as this depended on various factors such as the size of the organisation, cost, Cloud strategy, Cloud model, and Cloud service that is being consumed. Therefore, another recommendation will be to investigate the percentage of IT security professionals affected by the adoption of Cloud as well as quantifying Cloud-based newly created roles, and the jobs that have become irrelevant or redundant. Such a study will cover the population with a wide range of participants in terms of size and type of industry. It will give better perspective on the overall impact of the Cloud on the changing job roles and skills. Also, it will examine and quantify which type of organisation and industry will more likely to gain bigger advantages.

Furthermore, a future recommendation for this study would be to explore the difference each Cloud service (SaaS, IaaS, PaaS) make to the skill sets and organisational requirements. The type of Cloud service determines the skills and roles required for the Cloud model for an organisation. Security and organisation's responsibility differs greatly between Cloud services, requiring different tasks, tools, policies and skills. Organisations will benefit more from understanding the skills requirement for specific Cloud service.

Another recommendation for the future development of this research is to investigate how organisational structure and strategy determine the impact Cloud has on security skills and roles. The literature outlines different factors that determine the extent of the impact of Cloud an organisation experience. Additional research in this

area can provide further insight. Furthermore, the findings show that where and how IT security skills are taught should be revised. More importantly, HEIs have a major role in managing rapid technological changes. Another future research recommendation building on this study would be to evaluate the actual changes or intentions to change, that have been made to the curriculum in the HEIs to meet the requirements of the cybersecurity industry.

REFERENCES

- Abba, M. (2018). Explored and Critique of Contingency Theory for Management Accounting Research. *Journal of Accounting and Financial Management*, 4(5), 40-50.
- Abbott, M. G. (1967). The Social Psychology of Organizations. *Educational Administration Quarterly*, 3(1), 100-109.
- Acemoglu, D., & Autor, D. (2011). Skills, tasks and technologies: Implications for employment and earnings. In *Handbook of labor economics* (Vol. 4, pp. 1043-1171): Elsevier.
- Adel, A., Reza, S., & David, J. (2013, November). Migration to Cloud Computing-The Impact on IT Management and Security. *Atlantis Press*. Symposium conducted at the meeting of the 1st International Workshop on Cloud Computing and Information Security, Shanghai, China. <https://doi.org/https://doi.org/10.2991/ccis-13.2013.46>
- Adolphus, M. (2011). How to undertake case study research. *Opgeroepen op mei*, 22, 2011.
- Adu, P. (2016). Perfecting the art of qualitative coding *QSR International* (Vol. 2020).
- AHPC. (n.d.) *The American Heritage Dictionary of the English Language*: Houghton Mifflin Harcourt Company.
- Al-Abbadi, S. A. (2015). Market environment and centralized decision-making and their impact on the effectiveness of organizations. *International Business Research*, 8(2), 129. <https://doi.org/10.5539/ibr.v8n2p129>
- Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*, 25(1), 107-136. <https://doi.org/https://doi.org/10.2307/3250961>
- Aliyu, A. A., Bello, M. U., Kasim, R., & Martin, D. (2014). Positivist and non-positivist paradigm in social science research: Conflicting paradigms or perfect partners. *J. Mgmt. & Sustainability*, 4(3), 79. <https://doi.org/https://doi.org/10.5539/jms.v4n3p79>
- Alliance, C. S. (n.d.). Retrieved February 4, 2021, 2021, from <https://cloudsecurityalliance.org/education/>
- Alosaimi, R., & Alnuem, M. (2016). Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 8(4). <https://doi.org/10.5121/ijcsit.2016.8401>
- Alter, S. (2000). *Information systems: A management perspective* (3rd ed.): Addison-Wesley Publishing Company.
- Anderson, C., & Gantz, J. F. (2012). *Climate change: Cloud's impact on IT organizations and staffing*. Framingham, MA, USA.
- Anderson, J. (2010). ICT transforming education-A Regional Guide: UNESCO Bangkok, Thailand.
- Aragón-Correa, J. A., & Sharma, S. (2003). A contingent resource-based view of proactive corporate environmental strategy. *Academy of management review*, 28(1), 71-88.
- Archer, M., Decoteau, C., Gorski, P., Little, D., Porpora, D., Rutzou, T., Smith, C., Steinmetz, G., & Vandenberghe, F. (2016). *What is critical realism?*

- Perspectives: A Newsletter of the ASA Theory Section, Fall 2017*. Retrieved 29/06/2020, 2020, from <http://www.asatheory.org/current-newsletter-online/what-is-critical-realism>
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . others. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.
- Arora, A. S., Raja, L., & Bahl, B. (2018). Data Centric Security Approach: A Way to Achieve Security & Privacy in Cloud Computing.
- Asatiani, A. (2016). Impact of Cloud Computing on Business Process Outsourcing-Case: Accounting in Small and Medium-sized Enterprises.
- Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. *IT professional*, 13(1), 12-15. <https://doi.org/doi.org/10.1109/MITP.2011.6>
- Atieno, O. P. (2009). An analysis of the strengths and limitation of qualitative and quantitative research paradigms. *Problems of Education in the 21st Century*, 13(1), 13-38.
- Auckland University of Technology, A. (n.d.). *Networks and Cybersecurity Major - Bachelor of Computer and Information Sciences*. Retrieved February 5, 2021, from <https://www.aut.ac.nz/study/study-options/engineering-computer-and-mathematical-sciences/courses/bachelor-of-computer-and-information-sciences/networks-and-cybersecurity-major-bachelor-of-computer-and-information-sciences>
- Avadikyan, A., Lhuillery, S., & Negassi, S. (2016). Technological innovation, organizational change, and product-related services. *M@n@gement*, 19(4), 277-304.
- Avedian, A. (2014). *Survey design*. Harvard Law School. Retrieved from <http://hnmcp.law.harvard.edu/wp-content/uploads/2012/02/Arevik-Avedian-Survey-Design-PowerPoint.pdf>
- Avram, M.-G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, 12, 529-534. <https://doi.org/doi.org/10.1016/j.protcy.2013.12.525>
- Axel, B., Boudhayan, C., Lennie, D.-B., Cesar, G., Brian, H., Madhukar, R. N., . . . Jan, T. (2014). *Reduce Risk and Improve Security on IBM Mainframes: Volume 1 Architecture and Platform Security* (Vol. 1): IBM Redbooks. Retrieved from <http://www.redbooks.ibm.com/abstracts/sg247803.html?Open>
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of management*, 17(1), 99-120. <https://doi.org/https://doi.org/10.1177/014920639101700108>
- Barrett, D. (2017). Applying a Contingency Framework to Digital Forensic Processes in Cloud Based Acquisitions. *Journal of Digital Forensics, Security and Law*, 12(2), 9.
- Baskarada, S. (2014). Qualitative case study guidelines. *Baškarada, S.(2014). Qualitative case studies guidelines. The Qualitative Report*, 19(40), 1-25.
- Baskerville, R., & Wood-Harper, A. T. (1998). Diversity in information systems action research methods. *European Journal of information systems*, 7(2), 90-107. <https://doi.org/> <https://doi.org/10.1057/palgrave.ejis.3000298>
- Bastedo, M. N. (2004). Open systems theory. from CiteSeerX <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.694.1365>

- Bauer, T. K., & Bender, S. (2004). Technological change, organizational change, and job turnover. *Labour Economics*, 11(3), 265-291.
<https://doi.org/https://doi.org/10.1016/j.labeco.2003.09.004>
- Bazeley, P., & Jackson, K. (2013). *Qualitative data analysis with NVivo* (2nd ed.): SAGE publications limited.
- Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3), 369-386.
<https://doi.org/10.2307/248684>
- Bento, A., & Bento, R. (2011). Cloud computing: A new phase in information technology management. *Journal of Information Technology Management*, 22(1), 39-46.
- Berghel, H. (2012). Identity theft and financial fraud: Some strangeness in the proportions. *Computer*, 45(1), 86-89.
- Bharadwaj, S. S., & Lal, P. (2012). Exploring the impact of Cloud Computing adoption on organizational flexibility: A client perspective *IEEE*. Symposium conducted at the meeting of the International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)
- Bhatia, M. (2018). Your guide to qualitative and quantitative data analysis methods.
- Bhatnagar, P. (2015). Cloud computing changes IT job roles: IBM.
- Bhattacharjee, A. (2012). *Social science research: Principles, methods, and practices* (2nd ed.). Retrieved from <https://open.umn.edu/opentextbooks/textbooks/79>
- Blackstone, A. (2018). Principles of sociological inquiry: Qualitative and quantitative methods.
- Bob, S., Geoff, V., & David, N. (2011). *Creating an effective hybrid IT model: What CIOs need to know*: Ernst & Young. Retrieved from <https://vdocuments.net/reader/full/creating-an-effective-hybrid-it-model-what-cios-need-to-know>
- Bogner, A., Littig, B., & Wolfgang, M. (2009). Introduction: Expert Interviews — An Introduction to a New Methodological Debate (pp. 1-13). London: Palgrave Macmillan, London.
- Bohm, M., Leimeister, S., Riedl, C., & Krcmar, H. (2010). *Cloud computing and computing evolution*. Germany: Technical University of Munich (TUM), Germany.
- Boillat, T., & Legner, C. (2013). From on-premise software to cloud services: the impact of cloud computing on enterprise software vendors' business models. *Journal of theoretical and applied electronic commerce research*, 8(3), 39-58.
- Bonello, M., & Meehan, B. (2019). Transparency and Coherence in a Doctoral Study Case Analysis: Reflecting on the Use of NVIVO within a 'Framework' Approach. *The Qualitative Report*, 24(3), 483-498.
- Bounagui, Y., Hafiddi, H., & Mezrioui, A. (2014). Challenges for IT based cloud computing governance *IEEE*. Symposium conducted at the meeting of the International Conference on Intelligent Systems: Theories and Applications (SITA-14) <https://doi.org/doi.org/10.1109/SITA.2014.6847289>
- Bounfour, A., Fernandez, V., & Waller, E. (2015). Cloud computing and organisational design: towards a comprehensive research agenda. *Systemes d'information management*, 20(4), 3-10.

- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, 9(2), 27-40.
- Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, risk, and compliance in cloud scenarios. *Applied Sciences*, 9(2), 320. <https://doi.org/https://doi.org/10.3390/app9020320>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101.
- Bricki, N., & Green, J. (2007). *A guide to using qualitative research methodology*. Retrieved from https://evaluation.msf.org/sites/evaluation/files/a_guide_to_using_qualitative_research_methodology.pdf
- Brooks, D. C. (2015). *The Changing Face of IT Service Delivery in Higher Education: EDUCAUSE*. Retrieved from <https://library.educause.edu/~media/files/library/2015/5/ers1501b.pdf?la=en>
- Brown, A., Zonooz, Piyum, Adebambo, Temi, Hammer, Josh, Parupalli, Sasikumar. (2019). *Achieving cyber governance risk & compliance in the cloud : A closer look at Amazon Web Services*: Deloitte. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-achieving-cyber-governance-risk-and-compliance-in-the-cloud.pdf>
- Brush, T. H., & Artz, K. W. (1999). Toward a contingent resource-based theory: the impact of information asymmetry on the value of capabilities in veterinary medicine. *Strategic Management Journal*, 20(3), 223-250.
- Cao, G., Wiengarten, F., & Humphreys, P. (2011). Towards a contingency resource-based view of IT business value. *Systemic Practice and Action Research*, 24(1), 85-106.
- Carcary, M. (2009). The Research Audit Trial--Enhancing Trustworthiness in Qualitative Inquiry. *Electronic Journal of Business Research Methods*, 7(1).
- Carraway, D., Michael Cato, Mike Chapple, Alan Crosswell, Tom Dugas, Bob Flynn, Chad Haffenden, Sharon Pitt, Kim Round, Miguel Soldi, Oren Sreebny, Steve Terry, Thomas Trappler, Joseph Vaughan, Bruce Vincent, Bill Wroblewski, Gabe Youtsey. (2015). *Transforming the IT organization*: EDUCAUSE Center for Analysis and Research. Retrieved from <https://library.educause.edu/~media/files/library/2015/5/ewg1509-pdf.pdf>
- Caruana, E. J., Roman, M., Hernández-Sánchez, J., & Solli, P. (2015). Longitudinal studies. *Journal of thoracic disease*, 7(11), E537-E540. <https://doi.org/10.3978/j.issn.2072-1439.2015.10.63>
- Cascio, W. F., & Montealegre, R. (2016). How technology is changing work and organizations. *Annual Review of Organizational Psychology and Organizational Behavior*, 3, 349-375.
- Casula, M., Rangarajan, N., & Shields, P. (2020). The potential of working hypotheses for deductive exploratory research. *Quality & Quantity*, 1-23.
- CDCP. (2019). *The importance of KSA's (knowledge, skills and abilities) in the federal application process*. GA, USA: Centers for Disease Control and Prevention Human Resource Management Office Retrieved from <https://www.cdc.gov/hrmo/ksahowto.htm>

- Chen, D., & Stroup, W. (1993). General system theory: Toward a conceptual framework for science and technology education for all. *Journal of Science Education and Technology*, 2(3), 447-459.
- Chen, Y., Paxson, V., & Katz, R. H. (2010). *What's new about cloud computing security*: EECS Department, University of California, Berkeley. Retrieved from <http://www2.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf>
- Cheon, M. J., Grover, V., & Teng, J. T. (1995). Theoretical perspectives on the outsourcing of information systems. *Journal of information Technology*, 10(4), 209-219.
- Cherdantseva, Y., & Hilton, J. (2012). The Evolution of Information Security Goals from the 1960s to today.
- Chigbu, U. E. (2019). Visually hypothesising in scientific paper writing: Confirming and refuting qualitative research hypotheses using diagrams. *Publications*, 7(1), 22.
- Child, J. (1975). Managerial and organizational factors associated with company performance-part II. A contingency analysis. *Journal of Management Studies*, 12(1-2), 12-27.
- Chilisa, B., & Kawulich, B. (2012). Selecting a research approach: paradigm, methodology and methods. *Doing Social Research, A Global Context*. London: McGraw Hill.
- Chiregi, M., & Navimipour, N. J. (2017). A comprehensive study of the trust evaluation mechanisms in the cloud computing. *Journal of Service Science Research*, 9(1), 1-30.
- Christensen, C. (2002). The rules of innovation. *Technology Review*, 105(5), 32-38.
- Christiansen, C. (1997). The innovator's dilemma. *Harvard Business School Press, Boston*.
- Chukwudi, I., Zhang, M., & Gable, G. (2019). Extensive Theory Testing Using Case Study Symposium conducted at the meeting of the International Conference on Information Systems (ICIS), Munich, Germany Retrieved from <https://eprints.qut.edu.au/136915/1/136915.pdf>
- Chutikulrungeee, T. (2020). *A phenomenological study of other-generated disclosure in online social networks* (Doctor of Philosophy). Charles Sturt University, Australia.
- Ciborra, C. U. (2009). The platform organization: Recombining strategies, structures, and surprises. In *Bricolage, Care and Information* (pp. 134-158): Springer.
- CIGREF. (2011). *Information systems roles in large companies HR Nomenclature*: CIGREF. Retrieved from https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/2011_IS_roles_in_large_companies_HR_nomenclature_CIGREF_EN.pdf
- Cisco. (n.d.). *CCNA Cloud*. Retrieved February 4, 2021, from <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-cloud.html#~recertification>
- Cisco. (n.d.). *CCNP Cloud*. Retrieved February 4, 2021, from <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-cloud.html?dtid=osscdc000283>

- Clohessy, T. (2016). *The impact of cloud computing on IT service providers' business models*. National University of Ireland, Galway. Retrieved from <http://hdl.handle.net/10379/5620>
- Cobb, S. (2016). Mind this Gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis Symposium conducted at the meeting of the Virus Bulletin Conference
- Commission, N. P. (2019). *New Zealand, Technology and Productivity: technological change and the future of work (draft report 1)*: September, Wellington: New Zealand Productivity Commission.
- CompTIA. (2017). *The evolution security skills*: CompTIA. Retrieved from <https://www.comptia.org/content/research/the-evolution-of-security-skills>
- CompTIA. (2019). *CompTIA Cloud+Certification Exam Objectives*. Retrieved from https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-cloud-cv0-003-exam-objectives.pdf?sfvrsn=261b911_2
- Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering cybersecurity education in the US: an analysis of the critical factors *IEEE*. Symposium conducted at the meeting of the 2014 47th Hawaii International Conference on System Sciences
- Coovert, M. D., & Thompson, L. F. (2013). *The psychology of workplace technology* (1st ed.): Routledge.
- Cresswell, J. W. (2013). Philosophical Assumptions and Interpretive Frameworks. In J. W. Creswell (Ed.), *Qualitative inquiry & research design: choosing among five approaches* (Third edition ed., pp. 15-41). Thousand Oaks, California: SAGE Publications.
- Creswell, J. W. (2003). *Research design: qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA.: Sage Publications.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage publications.
- Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into practice*, 39(3), 124-130.
- Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*: Sage.
- Crumpler, W., & Lewis, J. A. (2019). *Cybersecurity Workforce Gap*: Center for Strategic and International Studies (CSIS).
- CSIS. (2016). *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills*: Center for Strategic and International Studies. Retrieved from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf>
- Culley, G., & Panteli, N. (2015). Exploring the Impact of Cloud Computing on IT Departments *Academic Conferences and publishing limited*. Symposium conducted at the meeting of the ECIME2015-9th European Conference on IS Management and Evaluation: ECIME 2015
- Cummings, T. G. (2015). Closed and Open Systems: Organizational. In J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)* (pp. 893-896). Oxford: Elsevier. Retrieved from <http://www.sciencedirect.com/science/article/pii/B978008097086873114X>.
<https://doi.org/https://doi.org/10.1016/B978-0-08-097086-8.73114-X>

- Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. *Communications of the ACM*, 53(4), 27-29.
- Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing*, 36(4), 253-263.
- Darity, W. A. (2008). Hypothesis and Hypothesis Testing *International Encyclopedia of the Social Sciences* USA: Macmillan Reference USA.
- Dawson, C. (2009). Introduction to Research Methods. A practical guide for anyone undertaking a research project, How to Content: Oxford, London.
- Dobson, P. J. (1999). Approaches to theory use in interpretive case studies—a critical realist perspective Symposium conducted at the meeting of the Australasian Conference on Information System, Wellington, New Zealand
- Draganidis, F., & Mentzas, G. (2006). Competency based management: a review of systems and approaches. *Information management & computer security*, 14(1), 51-64. <https://doi.org/https://doi.org/10.1108/09685220610648373>
- Driscoll, D. L. (2011). Introduction to primary research: Observations, surveys, and interviews. *Writing spaces: Readings on writing*, 2, 153-174.
- Ebbers, M., Bosch, W., Ebert, H. J., Hellner, H., Johnston, J., Kroll, M., . . . others. (2016). *Introduction to the New Mainframe: IBM Z/VSE Basics*: IBM Redbooks.
- Edhlund, B., & McDougall, A. (2019). *NVivo 12 essentials* (1st ed.): Lulu. com.
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, 14(4), 532-550.
- Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal*, 50(1), 25-32.
- Ellis, T. J., & Levy, Y. (2008). Framework of problem-based research: A guide for novice researchers on the development of a research-worthy problem. *Informing Science*, 11.
- Ertmer, P. A., & Ottenbreit-Leftwich, A. T. (2010). Teacher technology change: How knowledge, confidence, beliefs, and culture intersect. *Journal of research on Technology in Education*, 42(3), 255-284.
- Eyisi, D. (2016). The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum. *Journal of Education and Practice*, 7(15), 91-100.
- Fellows, W. (2008). Partly Cloudy, Blue-Sky Thinking About Cloud Computing. *Whitepaper*. 451 Group.
- Fernández, W. D. (2004). The grounded theory method and case study data in IS research: issues and design. In *Information Systems Foundations Workshop: Constructing and Criticising* (Vol. 1, pp. 43-59). Australia: The Australian National University Press.
- Filstead, W. J. (1979). Qualitative methods: A needed perspective in evaluation research. *Qualitative and quantitative methods in evaluation research*, 33-48.
- Fisher, T. (2014). *The CIO as Chief Innovation Officer: How Cloud Is Changing the CIO Role*. TX, USA: Outsourcing Center LLC & Oracle.
- Fitó, J. O., & Guitart Fernández, J. (2010). *Introducing risk management into cloud computing*: Barcelona Supercomputing Center and Technical University of Catalonia. Retrieved from <http://gsi.ac.upc.edu/reports/2010/33/cnsm10.pdf>

- Fletcher, M., & Plakoyiannaki, E. (2008). Case study selection: An overview of key issues for International Business Researchers *European International Business Academy (EIBA)*. Symposium conducted at the meeting of the Proceedings of the EIBA Annual Conference, Tallinn, Estonia.
- Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). *Cloud computing and grid computing 360-degree compared*. presented at the meeting of the Grid Computing Environments Workshop (GCE), Austin, TX. <https://doi.org/10.1109/GCE.2008.4738445>
- Frank, M. (2012). Don't get SMACKed: how social, mobile, analytics and cloud technologies are reshaping the enterprise. *Cognizant Future of Work*.
- Furht, B. (2010). Cloud computing fundamentals [furht2010cloud]. In *Handbook of cloud computing* (pp. 3-19): Springer.
- Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, 2017(2), 5-10.
- Galbraith, J. (1973). *Designing complex organizations*. Boston, MA United States: Addison-Wesley Longman.
- Garrison, G., Wakefield, R. L., & Kim, S. (2015). The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. *International Journal of Information Management*, 35(4), 377-393.
- Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The discovery of grounded theory; strategies for qualitative research. *Nursing research*, 17(4), 364.
- Gliner, J. A. (1994). Reviewing qualitative research: Proposed criteria for fairness and rigor. *The Occupational Therapy Journal of Research*, 14(2), 78-92.
- Göb, R., McCollin, C., & Ramalhoto, M. F. (2007). Ordinal methodology in the analysis of Likert scales. *Quality & Quantity*, 41(5), 601-626.
- Golson, J. P. (1977). The impact of technological change on organization management Symposium conducted at the meeting of the Proceedings of the 15th annual Southeast regional conference
- Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to Information Security—Public Health Implications. *New England Journal of Medicine*, 377(8), 707-709.
- Gorton, C. (2019). *IDC says New Zealand Organisations' Adoption of PaaS Solutions is Increasing*: International Data Corporation (IDC). Retrieved from <https://www.idc.com/getdoc.jsp?containerId=prAP45304819>
- Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse researcher*, 21(6).
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research*, 2(163-194), 105.
- Guide, Q. P. (2002). *Qualitative Data Processing*. UK. Retrieved from http://www.stis.ed.ac.uk/data/assets/word_doc/0009/13977/dataprocess.doc
- Guyette, S. (1983). *Community-based research: A handbook for Native Americans* (Vol. 1). LA, USA: American Indian Studies Center, University of California,.
- Hakim, Z. (2018). *Factors That Contribute to The Resistance to Cloud Computing Adoption by Tech Companies vs. Non-Tech Companies*. Nova Southeastern University, Fort Lauderdale, Florida, United States.

- Hancock, D. R., & Algozzine, B. (2017). *Doing case study research: A practical guide for beginning researchers*: Teachers College Press.
- Hanna, D. (1997). The organization as an open system. *Organizational effectiveness and improvement in education*, 13-21.
- Harding, J. (2018). *Qualitative data analysis: From start to finish*: SAGE Publications Limited.
- Harrell, M. C., & Bradley, M. A. (2009). *Data collection methods. Semi-structured interviews and focus groups*. CA USA: Rand National Defense Research Institute.
- Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case study research: foundations and methodological orientations. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 18(1). <https://doi.org/https://doi.org/10.17169/fqs-18.1.2655>
- Hedman, J., & Xiao, X. (2016). Transition to the Cloud: A Vendor Perspective/IEEE. Symposium conducted at the meeting of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA.
- Heltzel, P. (2015, 23/11/2018). Clouds ahead: What an IT career will look like five years out. Retrieved from <https://www.infoworld.com/article/2979872/clouds-ahead-what-an-it-career-will-look-like-five-years-out.html>
- Heron, R. (2005). *Job and work analysis: Guidelines on identifying jobs for persons with disabilities*. Geneva, Switzerland: International Labour Organization.
- Heublein, A. M. (2012). Open Source In The Clouds-How Organizational Ambidexterity Shapes and is Shaped by Disruptive Innovation in an Open Source Software Provider.
- Hilgendorf, K. (2016). *Analyzing the Role and Skills of the Cloud Architect*: Gartner Research Retrieved from https://www.gartner.com/binaries/content/assets/events/keywords/catalyst/cat-us8/analyzing_the_role_and_skills_of_cloud_architect.pdf
- Hipkins, R. (2006). *The nature of the key competencies: A background paper*. Wellington: New Zealand Council for Educational Research <https://doi.org/https://www.nzcer.org.nz/system/files/nature-of-k-round-paper.pdf>
- Hofer, C. W., & Schendel, D. (1978). *Strategy formulation: Analytical Concepts*. Minnesota, USA: West Publishing Company.
- Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243-248.
- Hox, J. J., & Boeijs, H. R. (2005). Data collection, primary versus secondary. *Encyclopedia of social measurement*, 1, 593-599.
- Huckvale, T., & Ould, M. (1995). Process modeling-who, what and how-role activity diagramming. *Business Process Change: Concepts, Methods and Technologies*, Idea Group Publishing, Harrisburg, PA, 330-349.
- Hughes, J. A., Randall, D., & Shapiro, D. (1992). From ethnographic record to system design. *Computer Supported Cooperative Work (CSCW)*, 1(3), 123-141.
- Hulley, S. B., Cummings, S. R., Browner, W. S., Grady, D. G., Hearst, N., & Newman, T. (2001). Conceiving the research question. *Designing clinical research*, 335.

- Huselid, M. A. (1995). The impact of human resource management practices on turnover, productivity, and corporate financial performance. *Academy of management journal*, 38(3), 635-672.
- Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International journal of qualitative studies on health and well-being*, 9(1), 23606.
- IBM. (2010). *Cloud for retail*. Somers, NY U.S.A.
- Irwin, S. (2013). Qualitative secondary data analysis: Ethics, epistemology and context. *Progress in development studies*, 13(4), 295-306.
- ISACA. (n.d.). *Certified in Risk and Information Systems Control (CRISC) certification*. Retrieved February 4, 2021, from <https://www.isaca.org/credentialing/crisc>
- ISACA. (n.d.). *Certified Information Systems Auditor (CISA) certification*. Retrieved February 4, 2021, from <https://www.isaca.org/credentialing/cisa>
- ISC2. (2020). *Certified Information Systems Security Professional(CISSP) Certification Exam Outline*. Retrieved from <https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CISSP-Exam-Outline-English-April-2021.ashx>
- ISC2. (n.d.). *CCSP Training Course Outline*. Retrieved February 4, 2021, from <https://www.isc2.org/Training/Courses/ccsp-training-course>
- ITU-T. (2008). *Overview of Cybersecurity*. Geneva, Switzerland
- Jabar, M. A., Sidi, F., Selamat, M. H., Ghani, A. A. A., & Ibrahim, H. (2009). An investigation into methods and concepts of qualitative research in information system research. *Computer and information Science*, 2(4), 47.
- Jadeja, Y., & Modi, K. (2012). Cloud computing-concepts, architecture and challenges Symposium conducted at the meeting of the Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on
- Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday*, 14(5).
- Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, 5(4), 87-88.
- Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 11(2).
- Jansen, W. (2011). Cloud hooks: Security and privacy issues in cloud computing *IEEE*. Symposium conducted at the meeting of the 44th Hawaii International Conference on System Sciences, Kauai, HI.
- Jebble, S., Dubey, R., Childe, S. J., Papadopoulos, T., Roubaud, D., & Prakash, A. (2018). Impact of big data and predictive analytics capability on supply chain sustainability. *The International Journal of Logistics Management*.
- Johnson, R., Thatcher, J., & Burleson, J. (2016). A framework and research agenda for studying eHRM: Automating and informing capabilities of HR technology. *Research in human resource management: Human resource management theory and research on new employment relationships*. Charlotte, NC: Information Age.

- Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer Law & Security Review*, 25(3), 270-274.
- Kabir, S. M. (2016). Formulating and testing hypothesis. In *Basic guidelines for research: An introductory approach for all disciplines*. (1st ed., pp. 51-71). Chittagong, Bangladesh: Book Zone Publication.
- Kaboub, F. (2008). Positivist paradigm. *Encyclopaedia of Counselling*, 2(2), 343.
- Kalchschmidt, M. (2012). Best practices in demand forecasting: Tests of universalistic, contingency and configurational theories. *International Journal of Production Economics*, 140(2), 782-793.
- Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS quarterly*, 571-586.
- Kaplan, B., & Maxwell, J. A. (2005). Qualitative research methods for evaluating computer information systems. In *Evaluating the organizational impact of healthcare information systems* (pp. 30-55): Springer.
- Katz, D., & Kahn, R. L. (1966). *The social psychology of organizations*. Wiley Oxford, England.
- Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management*, 32(5), 232-240.
- Khajeh-Hosseini, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2012). The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise. *Software: Practice and Experience*, 42(4), 447-465.
- Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT professional*, 12(5), 20-27.
- Khan, N., & Forshaw, T. (2017). *New Skills Now: Inclusion In The Digital Economy*. UK: Accenture.
- Killam, L. (2013). *Research terminology simplified: Paradigms, axiology, ontology, epistemology and methodology* (1st ed.). Ontario, Canada: Laura Killam.
- Kivunja, C., & Kuyini, A. B. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5), 26-41.
- Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, 24(1), 120-124.
- Kraaijenbrink, J., Spender, J.-C., & Groen, A. J. (2010). The resource-based view: A review and assessment of its critiques. *Journal of management*, 36(1), 349-372.
- Krikos, A. C. (2010). *Disruptive technology business models in cloud computing*. Massachusetts Institute of Technology.
- Kroonenburg, S. (2020). It's Time For Four-Year Universities To Teach Cloud Skills *Innovation* (Vol. 2020): Forbes Technology Council.
- Krusenvik, L. (2016). *Using Case Studies as a Scientific Method: Advantages and Disadvantages*: Halmstad University, Halmstad, Sweden.
- Kvale, S. (2006). Dominance through interviews and dialogues. *Qualitative inquiry*, 12(3), 480-500.
- Lane, P. (2020). CompTIA Security+ 501 vs. 601: What's the Difference? : CompTIA.
- Laugesen, N. S., Lauritzen, J. R., Carpenter, G., Ellegaard, C. E., Bucher, M., & Stabe, M. (2012). *Cloud Computing*.

- Lawrence Neuman, W. (2014). *Social research methods: Qualitative and quantitative approaches* (8th ed.). London, UK: Pearson Education, Limited.
- Leedy, P. D., & Ormrod, J. E. (2014). *Practical research: Planning and design*: Pearson Education.
- Leopold, T. A., Ratcheva, V., & Zahidi, S. (2018). The future of jobs report 2018 Symposium conducted at the meeting of the Geneva: World Economic Forum
- Lester, S. (1999). An introduction to phenomenological research: Taunton UK: Stan Lester Developments.
- Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care*, 4(3), 324.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newberry Park: CA: Sage.
- Ling-Yee, L. (2007). Marketing resources and performance of exhibitor firms in trade shows: A contingent resource perspective. *Industrial Marketing Management*, 36(3), 360-370.
- Littig, B., & Vienna, I. (2013). Expert Interviews. Methodology and Practice. *IHS Vienna, IASR lecture series, Vienna*.
- Ma, Q., & Ratnasingam, P. (2008). Factors affecting the objectives of information security management AIS. Symposium conducted at the meeting of the The International Conference on Information Resources Management (Conf-IRM), Ontario, Canada. Retrieved from <https://aisel.aisnet.org/confirm2008/29>
- Majumdar, S., Madi, T., Jarraya, Y., Pourzandi, M., Wang, L., & Debbabi, M. (2018). Cloud security auditing: Major approaches and existing challenges. *Springer*. Symposium conducted at the meeting of the International Symposium on Foundations and Practice of Security Retrieved from <https://dl.acm.org/doi/fullHtml/10.1145/1721654.1721672>
- Mangan, J., Lalwani, C., & Gardner, B. (2004). Combining quantitative and qualitative methodologies in logistics research. *International journal of physical distribution & logistics management*, 34(7), 565-578.
- Marquis, H. (2018). *The Impact of Cloud Computing on Staffing*. Retrieved from <https://www.globalknowledge.com/us-en/resources/case-studies/the-impact-of-cloud-computing-on-staffing/>
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision support systems*, 51(1), 176-189.
- Massey University, P. N. (n.d.). *Bachelor of Information Sciences (Information Technology)*. Retrieved February 5, 2021, from https://www.massey.ac.nz/massey/learning/programme-course/programme.cfm?major_code=PINTC&prog_id=93068
- Mathers, N., Fox, N., & Hunn, A. (1998). *Trent focus for research and development in primary health care: Using interviews in a research project* (2nd ed.). UK: Trent Focus Group.
- Matsuo, M., Wong, C. W., & Lai, K.-h. (2008). Experience-based learning of Japanese IT professionals: A qualitative research. *The Journal of Strategic Information Systems*, 17(3), 202-213.
- McKay, J., & Marshall, P. (2001). The dual imperatives of action research. *Information Technology & People*, 14(1), 46-59. <https://doi.org/https://doi.org/10.1108/09593840110384771>

- McKendrick, J. (2012). Majority of Companies Expanding Cloud Computing Skills: Survey. *Forbes*. Retrieved from <https://www.forbes.com/sites/joemckendrick/2012/07/24/majority-of-companies-expanding-cloud-computing-skills-survey/#611e79fc7c0d>
- Meijer, P. C., Verloop, N., & Beijaard, D. (2002). Multi-method triangulation in a qualitative study on teachers' practical knowledge: An attempt to increase internal validity. *Quality and quantity*, 36(2), 145-167.
- Mell, P., Grance, T., & others. (2011). *The NIST definition of cloud computing*. USA: National Institute of Standards and Technology (NIST).
- Mertler, C. (2016). Quantitative research methods. *Introduction to educational research*, 107-143.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand oaks, California: sage publications.
- Mitra, A., O'Regan, N., & Sarpong, D. (2018). Cloud resource adaptation: A resource based perspective on value creation for corporate growth. *Technological Forecasting and Social Change*, 130, 28-38.
- Mofaddel, M., & Tavangarian, D. (1997). *A Distributed System with a Centralized Organization*. Rostock, Germany: University of Rostock.
- Mokyr, J., Vickers, C., & Ziebarth, N. L. (2015). The history of technological anxiety and the future of economic growth: Is this time different? *Journal of Economic Perspectives*, 29(3), 31-50.
- Moore, F. I. (1999). Functional job analysis: guidelines for task analysis and job design. *World Health Organization. Department of Health Service Provision*.
- Morgan, S. (2017). *Cybercrime Report*. NY, USA: Cybersecurity Ventures and Herjavec Group. Retrieved from <https://www.herjavecgroup.com/wp-content/uploads/2018/07/2017-Cybercrime-Report.pdf>
- Mowbray, M. (2009). The fog over the grimpen mire: cloud computing and the law. *scripted*, 6, 132.
- Myers, M. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, 21(2), 241-242.
- Myers, M. D. (1999). Investigating information systems with ethnographic research. *Communications of the AIS*, 2.
- Myers, M. D. (2019). *Qualitative research in business and management* (3rd ed.). London: Sage Publications
- Nadler, D. A., & Tushman, M. L. (1980). A model for diagnosing organizational behavior. *Organizational Dynamics*, 9(2), 35-51.
- NCSS. (2018). *Initial National Cyber Security Skills Strategy - Increasing The Uk's Cybersecurity Capability*. UK: HM Government. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf
- Nemati, A. R., Bhatti, A. M., Maqsal, M., Mansoor, I., & Naveed, F. (2010). Impact of resource based view and resource dependence theory on strategic decision making. *International Journal of Business and Management*, 5(12), 110.
- Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An introduction to information security*: National Institute of Standards and Technology.

- Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, 18(2), 34-35. <https://doi.org/http://dx.doi.org/10.1136/eb-2015-102054>
- Nübler, I. (2016). New technologies: A jobless future or golden age of job creation. *International Labour Office Research Department Working Paper*, 13.
- O'Reilly, M., & Kiyimba, N. (2015). *Advanced qualitative research: A guide to using theory*. London: Sage Publications. Retrieved from <http://hdl.handle.net/10034/620998>
- Opala, O. J. (2012). *An analysis of security, cost-effectiveness, and it compliance factors influencing cloud adoption by it managers*. Capella University.
- Orlikowski, W. J. (1991). Integrated information environment or matrix of control?: The contradictory implications of information technology.
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, 2(1), 1-28.
- Padgett, D. (2017). Choosing the right qualitative approach (es). *Qualitative methods in social work research*, 31-56.
- Parker, C. M., Wafula, E. N., Swatman, P. M., & Swatman, P. A. (1994). Information systems research methods: The technology transfer problem Symposium conducted at the meeting of the Proceedings of the 5th Australian Conference on Information System
- Patel, S. (2015). The research paradigm–methodology, epistemology and ontology–explained in simple language. July 15th. Available at: <http://salmapatel.co.uk/academia/the-research-paradigm-methodologyepistemology-and-ontology-explained-in-simple-language> (Accessed: 1/6/17).
- Patton, M. Q., & Cochran, M. (2002). A guide to using qualitative research methodology. Retrieved with permission by Nouria Brikci-Research Officer, MSF UK (February 2007) http://evaluation.msf.at/fileadmin/evaluation/files/documents/resources_MSF/MSF_Qualitative_Methods.pdf.
- Paulsen, C. (2018). *Glossary of Key Information Security Terms*: National Institute of Standards and Technology.
- Peake, C. (2018). *Accepting the Cloud: A Quantitative Predictive Analysis of Cloud Trust and Acceptance Among IT Security Professionals*. Capella University, Minnesota, USA.
- Pechardscheck, S., & Christoph, S. (2012). *In Cloud we trust?*: BearingPoint Institute. Retrieved from <https://www.bearingpoint.com/en/our-success/thought-leadership/in-cloud-we-trust/>
- Pereira, R., Almeida, R., & da Silva, M. M. (2013). How to generalize an information technology case study *Springer*. Symposium conducted at the meeting of the International Conference on Design Science Research in Information Systems, Helsinki, Finland. https://doi.org/https://doi.org/10.1007/978-3-642-38827-9_11
- Perry, C. (1998). Processes of a case study methodology for postgraduate research in marketing. *European journal of marketing*, 32(9/10), 785-802. <https://doi.org/https://doi.org/10.1108/03090569810232237>

- Peshkin, A. (1993). The goodness of qualitative research. *Educational researcher*, 22(2), 23-29.
- Petroni, A. (1999). Managing information systems' contingencies in banks: a case study. *Disaster Prevention and Management: An International Journal*, 8(2), 101-110.
- Pieters, W. (2011). The (social) construction of information security. *The Information Society*, 27(5), 326-335.
- Ponelis, S. R. (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(1), 535-550.
- Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of counseling psychology*, 52(2), 126.
- Prasad, S., Rao, A., & Rehani, E. (2001). *Developing hypothesis and research questions*. Retrieved from <https://www.public.asu.edu/~kroel/www500/hypothesis.pdf>
- Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015). Cloud computing features, issues, and challenges: a big picture Symposium conducted at the meeting of the Computational Intelligence and Networks (CINE), 2015 International Conference on Abstract retrieved from puthal2015cloud
- Qiu, M., Gai, K., Thuraisingham, B., Tao, L., & Zhao, H. (2018). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Generation Computer Systems*, 80, 421-429.
- Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative research in accounting & management*, 8(3), 238-264.
- Radermacher, A., & Walia, G. (2013). Gaps between industry expectations and the abilities of graduates. *Association for Computing Machinery, New York*. Symposium conducted at the meeting of the ACM technical symposium on Computer science education, Denver Colorado USA. <https://doi.org/https://doi.org/10.1145/2445196.2445351>
- Rajendran, S. (2013). *Organizational challenges in cloud adoption and enablers of cloud transition program*. Massachusetts Institute of Technology.
- Rawal, B. S., Vijayakumar, V., Manogaran, G., Varatharajan, R., & Chilamkurti, N. (2018). Secure disintegration protocol for privacy preserving cloud storage. *Wireless Personal Communications*, 1-17.
- Restuccia, D., & Taska, B. (2018). Different Skills, Different Gaps: Measuring and Closing the Skills Gap. *Developing Skills in a Changing World of Work: Concepts, Measurement and Data Applied in Regional and Local Labour Market Monitoring Across Europe*, 207.
- Ridder, H.-G. (2017). The theory contribution of case study research designs. *Business Research*, 10(2), 281-305.
- Robb, T. (2011). Cloud computing winners and losers (Vol. 2018).
- Robb, T. (2011). Winners and Losers *Cloud computing series*: globalEdge Research.
- Rolfe, G. (2006). Validity, trustworthiness and rigour: quality and the idea of qualitative research. *Journal of advanced nursing*, 53(3), 304-310.

- Ross, P. (2011). How to keep your head above the clouds: Changing ICT worker skill sets in a cloud computing environment. *Employment Relations Record*, 11(1), 62. ross2011keep.
- Rowley, J. (2002). Using case studies in research. *Management research news*.
- Roy, K., & Khokhle, P. W. (2011). Integrating resource-based and rational contingency views: Understanding the design of dynamic capabilities of organizations. *Vikalpa*, 36(4), 67-76.
- Sandberg, J. (2005). How do we justify knowledge produced within interpretive approaches? *Organizational research methods*, 8(1), 41-68.
- Sanders, J. R. (2002). *A study of the relationship between organizational theories identified through the leadership beliefs and leadership behaviors of Indiana public school superintendents* (Ph.D.). Indiana State University, Ann Arbor. Available from ProQuest Dissertations & Theses Global database.
- SATI, M. (2018). Deloitte Insights TECH TRENDS 2018. *Tech Trends*, 151(162).
- Schwandt, T. A. (2001). *Dictionary of qualitative inquiry* (2nd ed.). Thousand Oaks, CA: SAGE.
- Scotland, J. (2012). Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, 5(9), 9.
- Seay, C., Washington, M., & Watson, R. J. (2016). Impact of the Cloud on IT Professionals and the IT Industry. *Encyclopedia of Cloud Computing*, 653-663. seay2016impact.
- Sepehr, H., & Aghapour, A. (2012). Insights into case-study: A discussion on forgotten aspects of case research. *International Journal of Scientific and Research Publications*, 2(3), 1-6.
- Shakir, M. (2002). The selection of case studies: strategies and their applications to IS implementation case studies. *Research Letters in the Information and Mathematical Sciences*, 3, 191-198.
- Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, 22(2), 63-75.
- Shorten, A., & Smith, J. (2017). Mixed methods research: expanding the evidence base. *Evidence Based Nursing*, 20(3), 74. <https://doi.org/10.1136/eb-2017-102699>
- Siggelkow, N. (2007). Persuasion with case studies. *Academy of management journal*, 50(1), 20-24.
- Silverstone, S., Phadungtin, J., & Buchanan, J. (2009). Technologies to Support Effective Learning and Teaching in the 21st Century. In *Advanced Technologies*: IntechOpen.
- Simon, M., & Goes, J. (2016). Reliability and Validity in Qualitative studies. <https://doi.org/https://doi.org/10.4102/curationis.v16i2.1396>
- Sincero, S. M. (2016). Types of survey (Vol. 2020): Explorable.
- Singel, R. (2011). Dropbox Left User Accounts Unlocked for 4 Hours Sunday. *WIRED*. Retrieved from <https://www.wired.com/2011/06/dropbox-4/>
- Singh, S., & Bartolo, K. (2005). Grounded theory and user requirements: A challenge for qualitative research. *Australasian Journal of Information Systems*, 12(2).
- Smith, A., & Anderson, J. (2014). AI, Robotics, and the Future of Jobs. *Pew Research Center*, 6.

- Smith, A., & Anderson, J. (2014). *AI, Robotics, and the Future of Jobs*: Pew Research Center. Retrieved from www.pewresearch.org/wp-content/uploads/sites/9/2014/08/Future-of-AI-Robotics-and-Jobs.pdf+&cd=2&hl=en&ct=clnk&gl=nz
- Soiferman, L. K. (2010). *Compare and Contrast Inductive and Deductive Research Approaches*. U.S. Department of Education: University of Manitoba Retrieved from <https://files.eric.ed.gov/fulltext/ED542066.pdf>
- Son, I., Lee, D., Lee, J.-N., & Chang, Y. B. (2014). Market perception on cloud computing initiatives in organizations: An extended resource-based view. *Information & Management*, 51(6), 653-669.
- Srinivasamurthy, S., Liu, D. Q., Vasilakos, A. V., & Xiong, N. (2013). Security and Privacy in Cloud Computing: A Survey. *Parallel & Cloud Computing*, 2(4). srinivasamurthy2013security.
- Stake, R. (2005). Qualitative case studies. In D. N. K. L. Y. S.(Eds.) (Ed.), *The Sage handbook of qualitative research* (pp. 443-466): Sage publications Ltd.
- Stake, R. E. (1995). The art of case study research *Calif Sage*.
- Starbuck, W. (2003). The Origins of Organization Theory. In (pp. 143-182). <https://doi.org/10.1093/oxfordhb/9780199275250.003.0006>
- Steenkamp, A. L., & McCord, S. A. (2007). Approach to teaching research methodology for information technology. *Journal of Information Systems Education*, 18(2), 255.
- Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, 78, 964-975.
- Stjelja, M. (2013). *The case study approach: Some theoretical, methodological and applied considerations*. Australia: Defence Science and Technology Organisation Edinburgh (Australia) Land.
- Stone, D. L., Deadrick, D. L., Lukaszewski, K. M., & Johnson, R. (2015). The influence of technology on the future of human resource management. *Human Resource Management Review*, 25(2), 216-231.
- Suby, M., & Dickson, F. (2013). *(ISC)2 Global information security workforce study*. Clearwater, FL: Frost & Sullivan
- Suby, M., & Dickson, F. (2017). *Global information security workforce study - Benchmarking Workforce Capacity and Response to Cyber Risk*. Clearwater, FL.
- Sultan, N. v. d. B.-K., Sylvia. (2012). Organisational culture and cloud computing: coping with a disruptive innovation. *Technology Analysis & Strategic Management*, 24(2), 167-179.
- Suo, S. (2013). *Cloud implementation in organizations: Critical success factors, challenges, and impacts on the IT function*. The Pennsylvania State University.
- Synnott, W. R., & Gruber, W. H. (1981). *Information resource management: Opportunities and strategies for the 1980s*: Wiley New York ua.
- Tassabehji, R. (2005). Principles for managing information security. In *Encyclopedia of Multimedia Technology and Networking* (pp. 842-848): IGI Global.
- Taylor, C., & Gibbs, G. R. (2010). What is qualitative data analysis (QDA)? *Online QDA Web Site*.
- TCBC. (2016). *Cloud Skills Requirements and Development: A TCBC Best Practices Document*.

- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, 18(7), 509-533.
- Thomas, G. (2015). *How to do your case study* (2 ed.). London: Sage Publications.
- Thomas, P. Y. (2010). *Towards developing a web-based blended learning environment at the University of Botswana* (PhD Dissertation). University of Botswana
- Thorne, S. (2000). Data analysis in qualitative research. *Evidence-based nursing*, 3(3), 68-70. <https://doi.org/http://dx.doi.org/10.1136/ebn.3.3.68>
- Tsang, E. W. (2014). Case studies and generalization in information systems research: A critical realist perspective. *The Journal of Strategic Information Systems*, 23(2), 174-186.
- Turner-Bowker, D. M., Lamoureux, R. E., Stokes, J., Litcher-Kelly, L., Galipeau, N., Yaworsky, A., . . . Shields, A. L. (2018). Informing a priori Sample Size Estimation in Qualitative Concept Elicitation Interview Studies for Clinical Outcome Assessment Instrument Development. *Value in Health*, 21(7), 839-842. <https://doi.org/https://doi.org/10.1016/j.jval.2017.11.014>
- Twala, A., & Kekwaletswe, R. (2019). *Towards A Strategic Cloud Computing Framework: A South African Context*
https://doi.org/10.33965/is2019_201905L028
- University of Auckland, A. (n.d.). *Bachelor of Advanced Science (Honours) (BAdvSci(Hons)) specialising in Computer Science*. Retrieved February 4, 2021, from <https://www.auckland.ac.nz/en/study/study-options/find-a-study-option/computer-science/undergraduate/badvscihons-compsci-from-2019.html>
- University of Canterbury, C. (n.d.). *Computer Engineering- Course Information*. Retrieved February 5, 2021, 2021, from <https://www.canterbury.ac.nz/study/subjects/computer-engineering/>
- University of Canterbury, C. (n.d.). *Software Engineering - Course Information*. Retrieved from <https://www.canterbury.ac.nz/courseinfo/GetCourses.aspx?course=COSC131|DATA301|DATA430&format=s&subjectnames=Software%20Engineering|Computer%20Science|Computer%20Engineering>
- University of Otago, O. (n.d.). *Department of Computer Science - Papers*. Retrieved February 5, 2021, from <https://www.otago.ac.nz/computer-science/study/otago673578.html>
- University of Waikato, W. (n.d.). *Degree planner — Bachelor of Computer Science (BCompSc)*. Retrieved February 5, 2021, from <https://www.waikato.ac.nz/study/qualifications/bachelor-of-computer-science>
- University of Canterbury, C. (n.d.). *Computer Engineering*. Retrieved from <https://www.canterbury.ac.nz/study/subjects/computer-engineering/>
- Van Audenhove, L. (2007). Expert interviews and interview techniques for policy analysis. *Vrije University, Brussel* Retrieved May, 5, 2009.
- van de Weerd, I., Mangula, I. S., & Brinkkemper, S. (2016). Adoption of software as a service in Indonesia: Examining the influence of organizational factors. *Information & Management*, 53(7), 915-928. <https://doi.org/https://doi.org/10.1016/j.im.2016.05.008>

- Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A Break in the Clouds: Towards a Cloud Definition. *SIGCOMM Comput. Commun. Rev.*, 39(1), 50-55. Vaquero:2008:BCT:1496091.1496100.
- Vascellaro, J. (2009). Google discloses privacy glitch. *Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/BL-DGB-1214>
- Victor, R. S. (2020). Connectivity knowledge and the degree of structural formalization: a contribution to a contingency theory of organizational capability. *Journal of Organization Design*, 9(1), 1-22.
- Victoria University, W. (n.d.). *Bachelor of Engineering with Honours – BE(Hons) : Majoring in Cybersecurity Engineering*. Retrieved February 5, 2021, 2021, from <https://www.wgtn.ac.nz/explore/degrees/engineering/apply?major=cybersecurity-engineering>
- Victoria University, W. (n.d.). *Bachelor of Science – BSc : Majoring in Computer Science*. Retrieved February 5, 2021, from <https://www.wgtn.ac.nz/explore/degrees/science/requirements?major=computer-science>
- Visser, P. S., Krosnick, J. A., & Lavrakas, P. J. (2000). Survey research. In *Handbook of Research Methods in Social Psychology*. New York.: Cambridge University Press.
- von Solms, R., Van Der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management*, 26(3), 143-153.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, 10(1), 69-80.
- Walsham, G. (1995). The emergence of interpretivism in IS research. *Information systems research*, 6(4), 376-394.
- Wang, W., Duffy, A. H., & Haffey, M. (2007). A post-positivism view of function behaviour structure Symposium conducted at the meeting of the DS 42: Proceedings of ICED 2007, the 16th International Conference on Engineering Design, Paris, France, 28.-31.07. 2007
- Weber, K., & Otto, B. (2007). *A Contingency Approach to Data Governance*. presented at the meeting of the International Conference on Information Quality (ICIQ-07), Cambridge, Massachusetts.
- Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of management review*, 14(4), 490-495.
- Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems*, 48, 15-19.
- Wieringa, R. (2013). Case study research in information systems engineering Symposium conducted at the meeting of the Proceedings of the 25th International Conference on Advanced Information Systems Engineering
- Williams, C. (2007). Research methods. *Journal of Business & Economics Research (JBER)*, 5(3), 65-71. <https://doi.org/https://doi.org/10.19030/jber.v5i3.2532>

- Winkler, T., Goebel, C., Benlian, A., Bidault, F., & Günther, O. (2011). The impact of software as a service on IS authority—a contingency perspective *AIS Electronic Library (AISEL)*. Symposium conducted at the meeting of the The International Conference on Information Systems, ICIS 2011, Shanghai, China.
- Winterton, J., Delamare-Le Deist, F., & Stringfellow, E. (2006). *Typology of knowledge, skills and competences: clarification of the concept and prototype*: Office for Official Publications of the European Communities Luxembourg.
- Wood, S. (2017). *Required Skill Sets of Information Technology Workers in Managed Hosting Environments in Higher Education*. Baker College Michigan, ProQuest LLC, United State of America.
- Xie, X., Liu, R., Cheng, X., Hu, X., & Ni, J. (2016). Trust-Driven and PSO-SFLA based job scheduling algorithm on Cloud. *Intelligent Automation \& Soft Computing*, 22(4), 561-566.
- Xing, B., & Marwala, T. (2017). Implications of the fourth industrial age for higher education. *The Thinker Issue 73 Third Quarter 2017*.
- Yeboah-Boateng, E. O., & Essandoh, K. A. (2014). Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. *International Journal of Emerging Science and Engineering*, 2(4), 13-20.
- Yin, R. (1994). Case study research: design and methods (Vol. 5). Thousand Oaks, Carlifornia USA: Sage Publications.
- Yin, R. (2003). *Case study research: design and methods* (3rd ed.). Thousands Oak, CA.: Sage Publishers.
- Yin, R. (2009). *Case Study Research: Design and Methods* Thousand Oaks CA: Sage.
- Youseff, L., Butrico, M., & Da Silva, D. (2008). Toward a unified ontology of cloud computing Symposium conducted at the meeting of the Grid Computing Environments Workshop, 2008. GCE'08
- Zainal, Z. (2007). Case study as a research method. *Jurnal Kemanusiaan*(9), 1-6.
- Zaini, M. K., Masrek, M. N., Johari, M. K., Sani, A., & Anwar, N. (2018). Theoretical Modeling of Information Security: Organizational Agility Model based on Integrated System Theory and Resource Based View. *International Journal of Academic Research in Progressive Education and Development*, 7(3).
- Zavou, A. (2015). *Information Flow Auditing In the Cloud*. Columbia University, New York.

GLOSSARY

Ability: refers to the ability to perform an observable activity at a particular time that results in an output (CDCP, 2019).

Competency: an overall combination of tacit and explicit knowledge, behaviour, and skills, that provides an individual with the potential for effectiveness in task performance (Draganidis & Mentzas, 2006, p. 54).

Information Security: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability" (Nieles, Dempsey, & Pillitteri, 2017, p. 2).

Information system: "discrete set of information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (Paulsen, 2018).

Information Technology: "Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency" (Paulsen, 2018)

Knowledge: a state of understanding through experience or study for effective action (Alavi & Leidner, 2001, pp. 109-110)

Roles: "a collection of activities that are usually inclined to appropriate organisational responsibility that is generally carried out by an individual or group with some organisationally relevant responsibility (Huckvale & Ould, 1995)."


Resources: are assets controlled by an organisation to enable the organisation to develop and implement strategies that improve its efficiency and effectiveness (Barney, 1991, p. 101).

Skills: a consistent response that is based on a knowledge component to a particular set of situational criteria (Conklin et al., 2014).

Task: is a unit of work activity to produce an output or a product (Acemoglu & Autor, 2011, p. 2)

APPENDIX A

AUTEC Ethics Approval



Auckland University of Technology Ethics Committee (AUTEC)
Auckland University of Technology
D-88, Private Bag 92006, Auckland 1142, NZ
T: +64 9 921 9999 ext. 8316
E: ethics@aut.ac.nz
www.aut.ac.nz/researchethics

1 July 2019

Brian Cusack
Faculty of Design and Creative Technologies

Dear Brian

Re Ethics Application: 19/205 Impact of cloud computing on IT security skills and roles

Thank you for providing evidence as requested, which satisfies the points raised by the Auckland University of Technology Ethics Committee (AUTEC).

Your ethics application has been approved for three years until 1 July 2022.

Standard Conditions of Approval


1. The research is to be undertaken in accordance with the [Auckland University of Technology Code of Conduct for Research](#) and as approved by AUTEC in this application.
2. A progress report is due annually on the anniversary of the approval date, using form EA2, which is available online through <http://www.aut.ac.nz/research/researchethics>.
3. A final report is due at the expiration of the approval period, or, upon completion of project, using form EA3, which is available online through <http://www.aut.ac.nz/research/researchethics>.
4. Any amendments to the project must be approved by AUTEC prior to being implemented. Amendments can be requested using the EA2 form: <http://www.aut.ac.nz/research/researchethics>.
5. Any serious or unexpected adverse events must be reported to AUTEC Secretariat as a matter of priority.
6. Any unforeseen events that might affect continued ethical acceptability of the project should also be reported to the AUTEC Secretariat as a matter of priority.

Please quote the application number and title on all future correspondence related to this project.

AUTEC grants ethical approval only. If you require management approval for access for your research from another institution or organisation, then you are responsible for obtaining it. If the research is undertaken outside New Zealand, you need to meet all locality legal and ethical obligations and requirements. You are reminded that it is your responsibility to ensure that the spelling and grammar of documents being provided to participants or external organisations is of a high standard.

For any enquiries, please contact ethics@aut.ac.nz

Yours sincerely,



Kate O'Connor
Executive Manager
Auckland University of Technology Ethics Committee

Cc: adelamLadedokun@aut.ac.nz; Alan Litchfield

APPENDIX B

Online Survey Questions Part One

1. How do you find working in the Cloud compared to working in a traditional IT environment?

A screenshot of a web browser's address bar showing a search engine results page for "cloud computing". The address bar contains the text "cloud computing" and a search icon. Below the address bar, the search results are displayed, showing a list of links and snippets related to cloud computing.

***2. Did you find your previous IT security knowledge and skills efficient when you started working in the Cloud?**

- ☐ Yes
- ☐ No
- ☐ Not sure

Please provide details

***3. Do you think the type of Cloud or Cloud service determines the required IT security skills?**

- ☐ Yes
- ☐ No
- ☐ Don't know

Please provide details

***4. Do you think new skills are needed to cope in the Cloud environment?**

- ☐ Yes
- ☐ No
- ☐ Not sure

Please explain

***5. Have you undergone any training to be able to work efficiently with the Cloud? In your own view, what are the needed skills required to work in Cloud computing?**

A rectangular text input field with a light gray border and a white background. It has a small vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

***6. How difficult is it to find the skills required to work in Cloud computing?**

A rectangular text input field with a light gray border and a white background. It has a small vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

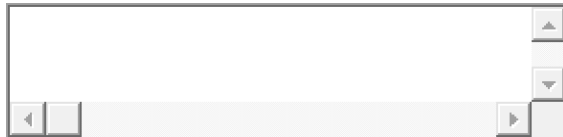
***7. Do you find some skills and job roles irrelevant in the Cloud?**

- ☐ Yes
- ☐ No
- ☐ Not sure

Please explain

A rectangular text input field with a light gray border and a white background. It has a small vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

***8. How is Cloud changing IT security job roles?**

A rectangular text input field with a light gray border and a white background. It has a small vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

***9. Do you think the Cloud is causing a significant change in the IT staffing model?**

- ☐ Yes
- ☐ No

Please provide details.

A rectangular text input field with a light gray border and a white background. It has a small vertical scrollbar on the right side and a horizontal scrollbar at the bottom.

***10. What is your own view are the general impact Cloud is having on IT security roles and skills, and how is this affecting the IT security jobs?**



APPENDIX C

Online Survey Questions Part Two

Question 1

***What is your job title?**

A rectangular text input field with a light gray border. On the right side, there are two small square buttons, one above the other, with upward and downward arrows. On the bottom left, there is a small square button with a left arrow, and on the bottom right, a small square button with a right arrow.

Question 2

***How many years have you been in the profession?**

- ☐ 0-3years
- ☐ 3-6years
- ☐ 7-10years
- ☐ 10+ years

Question 3

***How many years have you been in your current position?**

- ☐ 0-3years
- ☐ 3-6years
- ☐ 7-10years
- ☐ 10+ years

Question 4

***What type of Cloud service or environment is being deployed by your organisation?**

A rectangular text input field with a light gray border. On the right side, there are two small square buttons, one above the other, with upward and downward arrows. On the bottom left, there is a small square button with a left arrow, and on the bottom right, a small square button with a right arrow.

Question 5

***How long have your organisation been using Cloud services?**

- ☐ 0-3years
- ☐ 3-5years
- ☐ 5+ years

Question 6

To what extent do you agree or disagree with the following statements?

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
The basic or traditional IT security knowledge and skills are sufficient when working with Cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cloud has changed the skill sets required by IT security professionals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The type of Cloud deployed or Cloud service determines the skills sets of IT security professionals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Some IT skills will become irrelevant with the use of Cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The needed skills for IT security professionals are the same with or without Cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 7

***Please specify how much you agree or disagree with the following statements**

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly agree
Using Cloud services in an organisation changes the job roles/responsibilities of IT security professionals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The type of Cloud or Cloud service deployed determines the roles of IT security professionals	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>
Using Cloud services affect IT staffing in an organisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Some of the IT security job roles are becoming redundant	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 8

***Please describe how sufficient your previous IT security knowledge and skills were when you started working with Cloud?**

Question 9

***How has Cloud computing changed the roles/responsibilities of IT security professionals?**

Question 10

***How has Cloud computing changed the skill sets required by IT security professionals?**

Question 11

***How does the type of Cloud or Cloud service determine the skill sets and roles?**

Question 12

***How does Cloud computing affect IT staffing?**

Question 13

***What IT security job roles have changed in the Cloud environment**

Question 14

***What are the IT security skills needed to cope in a Cloud environment**

Question 15

If you would be willing to participate further in this research by taking part in a short chat (phone/skype/person) please put your email in the box below.

Question 16

Any further feedback?



APPENDIX D

Email Invitation

THE IMPACT OF CLOUD - INVITATION TO INTERVIEW

Dear participant,

I am contacting you because you've recently completed a survey on the impact of Cloud computing on IT security skills and roles. I will like to thank you for your contribution, your feedback is greatly appreciated.

The aim of the interview is to further explore the relationship between Cloud services, roles, and skills in the belief that Cloud services have brought about changes to the required security roles and skills.

The interview will take about 20-30 minutes of your time to capture your thoughts and opinions. Your participation in this research will provide insight into the changes in IT security roles and skills in organisations.

Please suggest a time and place that suits you. I understand you might be very busy, I'm flexible to do a phone or skype interview.

The participation and consent form has been attached for your information. Please let me know if you have any further questions or concerns

Thank you for your continued support in making this study a successful one.

Yours Sincerely,

Adekemi Adedokun,

Doctoral candidate,

Faculty of design and creative technologies,

AUT.

APPENDIX E

Follow up Email

Hi participant,

I am writing to follow-up on my email. I didn't hear back from you and I just want to check with you to be sure you received my email. It is regarding invitation for an interview for my study on the impact of Cloud computing on IT security skills and roles.

Please let me know when it will be convenient to have a quick chat with you. I have attached the participants and consent form for your information.

Regards,

Adekemi Adedokun,

Doctoral candidate,

Faculty of design and creative technologies,

AUT.