User Resistance to the Access Review Component of SailPoint IdentityIQ by Managers: A South African Bank Case Study

Submitted by:

Hangani Mudzunga

476167

In partial fulfilment of the requirements for the Degree of Master of Commerce in Information Systems

Supervised by:

Dr Emma Coleman

DECLARATION

I declare that this is my own unaided work and is, to the best of my knowledge and belief, original, except as acknowledged in the text.

I have read and understood the Senate policy on plagiarism and am aware that plagiarism is the intentional or unintentional "failure to acknowledge the ideas or writing of another" or "presentation of the ideas or writing of another as one's own". In this context "others" means any other person including a student, academic, professional, published author or other resource such as the internet. Failing to acknowledge the use of ideas of others constitutes an important breach of the values and conventions of the academic enterprise.

I am aware that plagiarism offences will be dealt with in terms of the Senate policy and may be subject to disciplinary action (which can result in dismissal from the course).

I have appended a reference list of citations used in this essay/assignment.

Date : 22 March 2022

Signature : 

Table of Contents

List of Figures

List of Tables

List of Appendix

ABSTRACT

The purpose of this study was to examine and explain why bank managers resist using the access review component of SailPoint IdentityIQ and explain the factors that influence bank managers to resist the access review component of SailPoint IdentityIQ. Moreover, the study also explained the managers' resistance behaviour.

The study adopted an interpretive paradigm and followed an inductive approach. Withing the broader scope of interpretive paradigm, the study adopted an explanatory research design. The case study strategy was employed by the study. Furthermore, the study employed a qualitative research method because its aim was not to generalise the research findings.

The time horizon for the study was cross-sectional, and the sources of the data for the study was the primary data source. This study's primary data collection method was interviews. Thematic analysis process was followed to analyse the data collected for the study.

The case study site was one of the South African banks, referred to in this study as ABC Bank. The research findings suggest that some bank managers at ABC bank do not perform access reviews mainly when their initial condition(s) and object(s) of resistance interact, they perceive something that leads them to behave in a resistant manner. Their perceptions are mostly on 1) whether they think they are doing something wrong, 2) ease of use, 3) consequences, 4) and value. These perceptions are developed by managers due to various factors such as fear of error, lack of perceived ease of use, lack of perceived consequences, and lack of perceived value.

The study contributed theoretically by following a different research methodology to explain user resistance in a different setting from that used previously in Lapointe and Rivard (2005) and Selander and Henfridsson (2012). The study followed a cross-sectional time horizon instead of a longitudinal time horizon, and it did so in a certain bank in South African. The study also tested the applicability of the Lapointe & Rivard (2005) framework in a South African bank following a qualitative methodology and cross-sectional time horizon. The study modified the Lapointe & Rivard (2005) framework to follow a qualitative methodology and cross-sectional time horizon to help answer the primary research question. The adaption of the framework proved to be helpful for the study.

The study also contributed to the user resistance, identity governance and administration body of knowledge in the information systems research because there is limited academic literature on subjects relating to the enterprise identity governance and administration systems.

Practically, the study contributes by providing some explanation on why some managers resist using the access review component of SailPoint IdentityIQ. The study also contributes by providing factors that influence managers not to perform access reviews on SailPoint IIQ. However, the author advises practitioners to generalise the findings of this study with caution. Moreover, the description reveals to practitioners that user resistance must be managed carefully by understanding the context as there is no 'silver bullet' strategy to mitigate user resistance.

LIST OF ABBRIVIATIONS

Acronym	**Details**
CIA	Confidentiality, Integrity, and Availability
IGA	Identity Governance and Administration
IIQ	IdentityIQ
HR	Human Resources
DOI	Diffusion of Innovation
TAM	Technology Acceptance Model
IT	Information Technology
MIS	Management Information System

CHAPTER 1: *INTRODUCTION*

This study examines and explains user resistance factors to a specific Identity Governance and Administration system component using a single case study. The element that is used for the study is the access review component of SailPoint IIQ. The study is conducted within the context of a South African bank.

The purpose of this chapter is to provide an overview of the study. The chapter will provide the study background, context, problem statement, purpose of the study, research questions, and an overview of the study's contribution to the body of knowledge.

1.1 Background

Confidentiality, integrity, and availability (CIA triad) are the core concepts of information security, *confidentiality* refers to the notion that access to information should be restricted to those individuals who have the correct privileges to access the information; *integrity* refers to the notion that modification of information should be restricted only to authorised individuals; and *availability* means that the systems and information should be available to authorised users when they are required (Ramluckan & Van Niekerk, 2014).

Information security is a combination of people, processes, and technology; the technological controls alone are not enough to mitigate threats to the information (Da Veiga & Eloff, 2007; Lopes & Oliveira, 2016). Lopes et al. (2017) define Information Security as a combination of processes aimed at securing information from different forms of threats to business continuity, reducing risks, and optimising returns on investments and business opportunities.

An information security management system is an approach that organisations follow to secure their information assets (Smedinghoff, 2008). It is a set of policies, processes, objectives, and systems (Kouns & Kouns, 2011; Smedinghoff, 2008).

Policies in information security refer to documents that depict top management's intention and direction regarding securing an organisation's information (Angraini et al., 2019). The documents encompass the security recommendations, rules, responsibilities and practices that an organisation adopt to secure information assets

(Angraini et al., 2019). Lack of information security policies and procedures makes an organisation vulnerable to information security threats (Peltier & Peltier, 2016).

Various technologies maintain confidentiality, integrity, and availability; this includes technologies such as Firewall, Socket Secure Layer, Access Control, Intrusion Detection, and Anti-Virus. These technologies achieve different objectives in the achievement and maintenance of the CIA triad. (Peltier & Peltier, 2016)

This study focuses on Access Control. Access control aims to allow authorised users access to organisational assets whilst restricting unauthorised users access to these assets (Rouhani et al., 2018). Access Control has two main types, that is logical access control and physical access control (Rouhani et al., 2018).

Logical Access Control refers to authorising or restricting users access to the organisation's network, systems, data, and other information assets (Rouhani et al., 2018). Physical Access Control refers to authorising or restricting users access to a physical location (Rouhani et al., 2018).

The interest of the study is on Logical Access Control. There are various forms of logical access control and the standard forms include software-based access control systems, firewall rules, and intrusion detection systems (Peltier & Peltier, 2016). However, all forms of access control have one objective which is to restrict or authorise user access to resources (Rouhani et al., 2018).

There are different access control mechanisms that organisations can apply. The commonly used mechanisms include Mandatory Access Control, Discretionary Access Control, Rule-Based Access Control, Role-Based Access Control, and Attribute-Based Access Control (Andress, 2011).

Mandatory Access Control is a mechanism that provides access based on the labels assigned to both the user requiring authorisation and the object being accessed (Andress, 2011; Zhang & Yang, 2003). Discretionary Access Control refers to a mechanism in which the object owner determines which users can access their object (Andress, 2011). Rule-Based Access Control is a mechanism that grants and restricts access based on conditions (Peltier & Peltier, 2016). Role-Based Access Control allows users access to objects based on their role within an organisation (Andress, 2011; Peltier & Peltier, 2016; Zhang & Yang, 2003). Attribute-Based Access Control is

a mechanism that grants and restricts access based on the attributes of a user, object, or environment (Andress, 2011).

The organisation must periodically review the access that users have to various information assets to ensure that only the authorised users have access to the information assets in question (ISO 27002, 2013). The periodic review of access is regardless of the mechanism that an organisation chooses to apply for controlling access to the information assets within an organisation.

Technology is paramount in maintaining data integrity, confidentiality, and availability and ensuring that the systems obey the laws and regulations (Peltier & Peltier, 2016). The technology that this study will primarily focus on is an Identity Governance and Administration system named SailPoint IdentityIQ. The Information Security policy should comprise the access management and periodic access rights review requirements. (ISO 27001, 2013).

The technological controls alone are not enough to mitigate threats to the information (Da Veiga & Eloff, 2007; Lopes & Oliveira, 2016). Organisations must also consider procedural and human behavioural components, these can be mitigated by use of security policies, standards, and guidelines. Additionally, organisations must also ensure that employees are aware of the security policies, standards, and guidelines (Da Veiga & Eloff, 2007). Identity Governance and Administration

Friedman (2018:3) defines Identity Governance and Administration as "technology and processes to ensure that people have appropriate access to applications and systems, and that the organisation always knows who has access to what, how that access can be used, and if that access conforms to policy."

Identity governance and administration are primarily concerned with access policies, user access provisioning, and analysing access rules, risks, and activities (Friedman, 2018). Management of access has become a challenging task for large enterprises, with many employees accessing multiple systems and data sources (Zhao & Johnson, 2010). Moreover, organisations struggle to ensure that employees only have access relevant to their day to day tasks, which increases the risk of data or information misuse by employees (Zhao & Johnson, 2010).

Cybercriminals and hackers now target individual’s identities because individuals are the ones that have access to the network and applications that they might need to

disrupt (Friedman, 2018). Multiple vendors offer identity governance and administration (IGA) solutions. However, the market leaders in the IGA space are SailPoint, Saviynt, IBM, Omada, and One Identity (Gaehtgens et al., 2019).

1.2 SailPoint IdentityIQ

SailPoint IdentityIQ (IIQ) is an enterprise user centric IGA solution. It enables organisations to manage, monitor, and govern access privileges that users have in various enterprise systems using a central platform (SailPoint, 2018). According to the 'Magic Quadrant for Identity Governance and Administration', SailPoint IIQ is a leading IGA solution (Gaehtgens et al., 2019).

SailPoint IIQ has four core modules, namely Compliance Manager, Lifecycle Manager, Password Manager, and File Access Manager (SailPoint, 2019).

The Compliance Manager module enables the automation of access certifications/reviews, policy management, and audit reporting to strengthen the organisations' compliance processes while enhancing how organisations govern identities (SailPoint, 2019).

The Lifecycle Manager module allows the organisation to manage user access changes through access requests and event-based requests. Password Manager module enables users to manage passwords to applications without being too reliant on the help desk. File Access Manager allows organisations to manage and govern access to file shares (SailPoint, 2019). The following section discusses the Access certification in detail.

1.3 Access Certification/Review

Access certification enables managers and asset owners to review and confirm users' access to various systems. The completion of Access Certification must be periodic and regular to ensure that identities have the proper access. (Gaehtgens et al., 2019)

The Identity Management Institute (2019) defines access certification as a continuous process where managers systematically review who has access to organisational resources to confirm the necessary access required to perform job functions and revoke the unauthorised access.

Atyam (2010) describes Access Rights Review as a process for ensuring that the users in an organisation have the access rights they require. Rigon et al. (2014) stipulate that

for an organisation to control users' access effectively, it should have a formal process whereby managers periodically review the access privileges of their subordinates.

Zhao and Johnson (2010) also highlighted that the necessity for organisations to conduct access reviews periodically is to ensure that the employees still have only the appropriate access they need to perform their daily tasks. According to Shabani et al. (2015), the primary goal of access reviews is to ensure that only the authorised personnel have access to the systems and information.

In this study, managers are individuals that have at least one subordinate reporting to them as per the Human Resource (HR) System. During an access rights review, managers either approve or revoke their subordinates' access in various systems. Moreover, if managers do not complete an access review, their subordinates' access get automatically removed by the System when the access review expires.

Digital identities are high targets of cybercriminals and hackers; it is more important to secure and govern them because compromised identities have played an enormous role in significant data breaches (Friedman, 2018). For example, if an attacker hacks a privileged identity, it becomes easier to disrupt an organisation because the attacker can get hold of privileged information, compromising the confidentiality, integrity, and availability of the data and information. However, if access gets reviewed regularly, users tend to have only necessary access (less privileged), and segregation of duties gets maintained. Therefore, attackers will find it harder to disrupt an entire organisation as the attacker will only have access to limited applications within the organisation (Friedman, 2018).

Access reviews rely primarily on the involvement of people (managers and resource owners). According to Friedman (2018), sometimes a manager is presented with access reviews, and they do not know what to do. The fact that the success of reviews relies heavily on people, managers not knowing what to do is one of the risks that could potentially lead to managers resisting to complete the access review.

This study defines access certification as reviewing users' access to various systems periodically or as raised by a mover process. This study refers to major South African retail banks as Nedbank, First National Bank, ABSA, and Standard Bank.

1.4 User Resistance

Research in information systems (Ali et al., 2016; Hirschheim & Newman, 1988; Juergens, 1977; Lapointe & Rivard, 2005; Markus, 1983; Rivard & Lapointe, 2012; Waddell & Sohal, 1998) acknowledged that change is inevitable and therefore planning for a change is essential because it assists the organisation to achieve the desired project outcomes. Furthermore, individuals are affected by changes in one way or another where some adopt and use the technology, some are indifferent about the technology, some do not use the system, and others are resistant to the technology (Rivard & Lapointe, 2012).

User resistance is among the crucial issues that need to be understood in Information Systems to develop appropriate means of responding (Rivard & Lapointe, 2012; Vrhovec, 2016). According to Hirschheim and Newman (1988), and Haddara and Moen (2017), user resistance is one of the significant contributors to information systems failures. However, user resistance is a complex multi-dimensional phenomenon which is not good or bad (Burnes, 2015; Hirschheim & Newman, 1988; Waddell & Sohal, 1998).

In information systems research, Klaus and Blanton (2010) define user resistance as the behavioural conduct to oppose the execution or usage of new information systems. According to Li et al. (2011) and Luftman et al. (2013), change management is a crucial information system management issue to deal with user resistance. Organisations apply different change management tools to manage and mitigate resistance by users (Ali et al., 2016). Nevertheless, organisations must first understand the source of resistance because there are multiple reasons for user resistance (Burnes, 2015). Furthermore, the resistance behaviours often differ per employee or group (Lapointe & Rivard, 2005). Therefore, user resistance is a crucial information system management issue that differs per organisation and individual, and different strategies should be applied per case to minimise its impact. Previous information systems research, such as that by Markus (1983), Lapointe and Rivard (2005), Kim and Kankanhalli (2009), and Merhi and Ahluwalia (2019) recognised that there are gaps in understanding the factors that influence user resistance to technology.

User resistance literature acknowledges that user resistance is complex and unique for each organisation, and there is no 'one-size-fits-all' strategy for curbing user

resistance (Ali et al., 2016). Therefore, to mitigate user resistance, it is essential to understand the sources of user resistance in the context of an organisation and individuals (Burnes, 2015; Rivard & Lapointe, 2012). There is limited literature that focuses on the factors influencing user resistance to a specific component or feature of an enterprise system, specifically an access review component of an IGA system.

In the information systems and technology industry, it is critical to identify the root cause of a problem to understand what causes the problem (Sikora et al., 2015) . Harkness et al. (1996) support the importance of identifying the root cause of an issue experienced in information systems and the field of technology. Therefore, understanding the underlying factors influencing bank managers not to use the access review component of SailPoint IIQ is critical In SailPoint IIQ, the most prominent role that managers play is performing access reviews and approving access requests.

The study defines user resistance as the actions of not using the component of the system by the users that are aware that they are supposed to use the component of the system as stated in ABC Bank's Information Security policy.

1.5 Purpose of the study

User resistance is one of the contributing factors to the success or failure of information systems implementation efforts (Hirschheim & Newman, 1988; Kim & Kankanhalli, 2009). An in-depth understanding of user resistance in the context of an environment in which the implementation took place is key to mitigating user resistance because the mitigation of user resistance often results in the objectives of the project or initiative manifesting (Selander & Henfridsson, 2012). The management of user resistance is crucial because, with careful management, it can also be utilised to better (improve) the implemented change; therefore, user resistance is not entirely a negative factor (Waddell & Sohal, 1998).

The purpose of this study is to examine and explain why some bank managers do not complete access reviews for their subordinates using the access review component of SailPoint IIQ. The study uses the user resistance lens to examine and explain the reasons why bank managers do not use the access review component of SailPoint IIQ. The case study draws these reasons from the various bank managers because managers are the ones that generally perform access reviews for their immediate subordinates.

Furthermore, the study focuses on all the types of access reviews that managers perform at ABC bank for logical access. Logical access reviews that managers perform are periodic and mover access reviews.

The study intends to achieve its purpose by following an interpretative paradigm using an explanatory research design. Furthermore, the study aims to contribute to the user resistance and IGA existing literature.

1.6 Problem background

The case site is one of the South African Banks that implemented SailPoint IIQ. Since the implementation of SailPoint IIQ at ABC bank, there were various change management initiatives such as communications, training, documentation, and workshops to upskill end-users on SailPoint IIQ and its capabilities. The initiatives were to manage user expectations, mitigate user resistance, get more end-users' buy-in, and obtain feedback from end-users regarding SailPoint IIQ.

SailPoint IIQ has been integrated with many systems within ABC bank to enable access management and governance, close audit findings, and comply with some industry-wide standards, laws, and regulations. Within ABC bank, SailPoint IIQ has become a platform for primarily managing users access and performing access reviews. ABC Bank's information security policy states that all applications' access must be reviewed at least once a year, and privileged access must be reviewed more regularly. When an application's access is not being reviewed according to the policy, this results in an audit finding against business clusters as it exposes the bank to identity-related threats.

The South African banking industry uses SailPoint IIQ as their identity and access governance or identity governance and administration solution (Davey, 2016). Evidence from three out of four South African banks that presented at the Johannesburg SailPoint Identity Day Conference shows that some managers within the Banks' employ do not complete access reviews on SailPoint IIQ (Meyer & Van Schalkwyk, 2018; Moyo 2019; Steyn & Espag 2019).

The same behaviour occurs at ABC bank. For the Access Reviews that managers have received since access reviews on SailPoint IIQ started, some bank managers have not been completing access reviews for their subordinates which result to ABC bank not having fully completed access reviews. It appears that this behaviour is typical across

the major retail banks in South Africa, and this behaviour opens the banks to cyber or identity-related threats and compliance risks.

According to de Villiers, Govender, and Madumo (2020), the South African Banking industry has many regulatory bodies. The Financial Sector Regulations Act of 2017 regulates the banks by regulating functions of the bank separately through laws and regulations tailored for those functions. In addition to the Financial Sector Regulations Act of 2017, some laws and regulations are essential to regulating the banking sector for example; Bank Act 94 of 1990, Mutual Banks Act 124 of 1993, Co-operative Banks Act 40 of 2007, South African Reserve Bank Act 90 of 1990, National Payments Systems Act 78 of 1998, Currency and Exchanges Act 9 of 1933, Financial Intelligence Centre Act 30 of 2001, Financial Advisory and Intermediary Services Act 37 of 2002, National Credit Act, Consumer Protection Act 68 of 2008, Financial Markets Act of 2012, and Protection of Personal Information Act 4 of 2013 (cited in de Villiers et al. , 2020).

The abovementioned acts govern most of the functions within the banks, and there is a high reliance on electronic systems. Failure to comply with some of the laws and regulations could result in banks being penalised financially by the regulatory bodies; for example, the South African Reserve Bank penalised the banks (GBS Mutual Bank, Habib Overseas Bank Limited, Investec Bank, The South African Bank of Athens Limited, Standard Chartered Bank, Socgen, and Absa Bank Limited) an amount of over R46 Million for non-compliance in the year 2016 (Fin24, 2016; Omarjee, 2017; Sikhakhane, 2016).

With the banks being highly regulated, it is paramount to secure the banking platforms necessary to maintain the confidentiality, integrity, and availability (CIA triad) of data and information assets. One of the ways of ensuring that the CIA triad is maintained is by ensuring completion of access reviews by managers to mitigate threats associated with an identity (Friedman, 2018). ABC Bank has implemented and enforces an Information Security Policy to ensure that the bank does not fall short with one or more regulatory bodies regarding matters concerning information security.

At ABC Bank, maintaining the CIA triad is guided by following a CIA rating framework. As per the CIA rating framework, the confidentiality attribute suggests that the information asset is accessible only by authorised individuals. An information asset's

confidentiality reflects how important preventing general or unauthorised access to the asset is to the organisation. There are multiple information assets within ABC bank whereby the unauthorised access and disclosure of information can adversely affect organisational operations, organisational assets, or individuals. Moreover, the information classifications within the information assets are unrestricted, internal only, confidential, and secret.

The information that is labelled as ‘unrestricted’ refers to the information that is already in the public domain. The information with a label of ‘internal-only’ refers to ABC Bank's internal operations or communications, which is of general relevance to all employees and appropriate for distribution throughout the organisation. Internal only information would not typically have any significant negative impact if disclosed to unauthorised personnel. However, it could provide knowledge of ABC Bank internal operations, which may not be appropriate for the public. Information that is labelled ‘confidential’ and ‘secret’ has restrictions even within the organisation, so it is critical for access to such information to be reviewed as the policy suggests.

Information labelled ‘confidential’ refers to proprietary information to the bank or relates to a sensitive or specific business process and is not appropriate for viewing by all employees. Confidential information might negatively impact if it were disclosed to unauthorised personnel, both internally and externally.

Information labelled ‘secret’ refers to information which unauthorised disclosure, even within the bank, may cause severe financial or reputational damage, significant loss of competitive advantage, or lead to regulatory sanction and legal actions.

The integrity attribute of the CIA rating framework suggests that the accuracy and completeness of the information should be always there; that is, information alterations must be authorised and known. Within ABC Bank, there are multiple information assets whereby the unauthorised and accidental alteration of the information can adversely affect organisational operations, organisational assets, or individuals.

The availability attribute of the CIA rating framework suggests that the information must be accessible and usable when required. There are multiple information assets within ABC bank whereby their disruption of access to or use of information or an information system can adversely affect organisational operations, organisational assets, or individuals.

It is, therefore, significant to understand why there are managers that are not using the access review component of SailPoint IIQ because such actions can adversely affect ABC Bank, and severely so.

1.7 Problem Statement

User resistance in Information Systems research has been studied for decades by various authors such as Markus (1983), Hirschheim and Newman (1988), Marakas and Homik (1996), Lapointe and Rivard (2005), Kim and Kankanhalli (2009), Klaus and Blanton (2010), Rivard and Lapointe (2012), and Ali et al. (2016). User resistance is a complex multi-dimensional phenomenon (Burnes, 2015; Hirschheim & Newman, 1988; Joshi, 1991; Waddell & Sohal, 1998). Some authors argue that user resistance is a significant contributor to information systems failures (Haddara & Moen, 2017; Waddell & Sohal, 1998).

However, some authors argue that it is not in itself good or bad (Hirschheim & Newman, 1988; Waddell & Sohal, 1998). Some authors argue that if there is the appropriate management of user resistance, it might ultimately lead to an increase in system adoption and usage (Burnes, 2015; Klaus & Blanton, 2010; Rivard & Lapointe, 2012).

Selander and Henfridsson (2012) stipulate that understanding user resistance in the context of an environment in which the implementation took place is key to mitigating user resistance. Some South African banking institutions are experiencing some level of user resistance to using the access review component of SailPoint IIQ (Meyer & Van Schalkwyk, 2018; Moyo, 2019). However, in the user resistance literature, there is limited literature that focuses on the resistance by managers towards the access review component of an IGA system, let alone SailPoint IIQ. Therefore, there is limited theoretical explanation of why some bank managers do not complete access reviews through an IGA System such as SailPoint IIQ. Consequently, banking institutions are proceeding to integrate new enterprise systems into SailPoint IIQ to manage and govern employees access in the hope that the managers will perform access reviews.

Moreover, managers not completing the access reviews compromises the CIA triad because some employees might end up with excess access that they no longer need. Therefore, if managers continue not to use the access review component of SailPoint IIQ, ABC Bank might end up experiencing adverse effects on its organisational

operations, organisational assets, individuals, or even suffering financial loss, reputational damage, loss of competitive advantage, regulatory sanctions, or legal actions.

1.8 Study Significance

The study revealed that the literature in existence is not enough to explain the user resistance exerted towards a specific component of the system, specifically the access review component of an IGA system. Chapter four provides details of the findings and analysis. Thus, the analysis of this study adds to the existing literature by identifying the factors that influence user resistance to an access review component of an IGA system, and more specifically in the banking sector. Therefore, the contribution of this study is divisible in two characteristics: practical, and literature.

1.8.1 Practical contribution

Practically, this study provides several factors influencing user resistance to the access review component of an IGA System. The study also presents an opportunity for organisations implementing or considering implementing an IGA solution that has an access review component to develop strategies that might mitigate the risk of user resistance towards an access review component from manifesting. Furthermore, the study also presents a similar strategy development opportunity to organisations that have implemented an IGA Solution with an access review component.

1.8.2 Literature contribution

This study contributes to the existing body of knowledge on information systems, information security, and identity governance and administration, and user resistance by identifying several factors influencing user resistance to the access review component of an IGA System. Furthermore, the study can (with caution) make pragmatic inferences of the user resistance exerted towards an access review component of an IGA system.

The study adopted a research framework traditionally for longitudinal studies and applied it in a cross-sectional study to examine and explain the user resistance towards an access review component of an IGA system. Therefore, this study contributes to the academic literature by testing the framework's applicability in studying user resistance towards an access review component of an IGA System. The study also

contribute to the Lapointe and Rivard (2005) framework by studying ‘Perception’ instead of ‘Perceived Threats’.

The study is also one of the few academic studies that enquired about identity governance and administration in general. It is also one of the few studies that investigates user resistance to a component of an IGA system. Therefore, in that regard, the study inherently contributes to the literature by providing some IGA descriptions and providing some user resistance descriptions concerning a component of an IGA system.

1.9 Assumptions

The study assumes that the study participants participated without feeling any obligation to the researcher. Furthermore, the study also assumes that the participants answered the interview questions honestly and openly. The participants answered the questions to the best of their knowledge. Moreover, the study assumes that the participants have performed access reviews on SailPoint IIQ, or they have seen the access reviews screens of SailPoint IIQ.

1.10 Scope of the study

The focus of the study is primarily to identify the reasons that make some bank managers resist the access review component of SailPoint IIQ. Due to the time constraints, the study focuses mainly on why some bank managers resist the access review component of SailPoint IIQ. Since there are limited academic studies around identity governance and administration and access reviews, the study borrows literature from the practice and information security research.

The study does not focus on the access review of physical access nor how the organisations can develop strategies to mitigate the resistance. However, when participants raised some strategy opinions to mitigate resistance, the researcher enquired about how not having the raised strategies impacts the resistance behaviour.

1.11 Research Questions

The primary and secondary research questions for the study are as follows.

1.11.1 Primary research question

Why do bank managers resist the use of the access certification component of SailPoint IIQ? **[Perception]**

1.11.2 Secondary research questions

- What influences bank managers not to perform access reviews?[1] **[Initial Conditions]**
- What do bank managers resist?[2] **[Object of Resistance]**
- How do bank managers behave towards the access review component of SailPoint IIQ? **[Resistance Behaviour]**

1.12 Conclusion

In this chapter, the study presented the background of the study and the purpose of the study. The study also depicted the background of the problem and articulated the problem statement and the significance of the study, the study assumptions, limitations, and the scope of the study. Furthermore, the research questions and the study's contribution to the body of knowledge was presented. In the next chapter, the study will discuss the literature that is relevant to the study.

[1] This question refers to the conditions that already exist within the organisation, employee, and system that can influence managers not to perform access reviews in SailPoint IdentityIQ.
[2] This question refers to the very thing or object that managers resist when it comes to performing access reviews on SailPoint IdentityIQ.

CHAPTER 2: *LITERATURE REVIEW*

2.1 Introduction

This chapter provides reviews the existing literature that informs this study. The study is about the resistance of a component (Access Review component) of an IGA System (SailPoint IIQ) by bank managers. Many researchers have studied user resistance, but there is little literature on the resistance of an Access Review component of an IGA system. Consequently, the study will examine the literature on user resistance from related schools of thought.

This chapter follows the following structure: first, the concepts of Identity Management and Identity Governance and Administration are reviewed. The concept of user resistance will be discussed in this chapter, and how to examine user resistance from different perspectives, followed by the types of resistance. The last section focuses on the theoretical underpinnings of the research.

2.2 Identity Governance and Administration

An identity is a grouping of qualities that characterise somebody from a system's perspective, and it can be linked directly to an actual human being (Neira, 2020).

Identity Governance which is used interchangeably with Identity Governance and Administration (IGA), is the technologies and processes that the organisations use to warrant that identities have appropriate access at any given time. Friedman (2018) emphasizes that employees, at any given time, should have the exact access that they need to perform their job functions and nothing more.

According to Friedman (2018), an IGA involves a minimum of three processes: policy modelling, user account provisioning, and access certifications. *Policy modelling* determines the access that identities should get based on the roles they play in the organisation. *User account provisioning* enables the management and approval of access requests to organisational resources mainly in an automated fashion and removes redundant access when individuals change roles or leave the organisation. *Access certifications* enable the organisations to regularly verify that identities' access is provided and managed following the organisational policy. The IGA solution that this study is inquiring about is SailPoint IIQ, and the solution does offer at least the three processes that Friedman (2018) suggests.

When an organisation is considering implementing or has implemented an IGA solution, an organisation must develop a strategic roadmap (Friedman, 2018). A roadmap helps organisations to articulate its vision and goals and present an organisation with an opportunity to identify needs and prioritise projects, moreover, a roadmap can be short-term or long-term depending on the needs (Garcia & Bray, 1997). An IGA roadmap is a long-term (18 to 24 months) plan that guides an organisation throughout an IGA journey, and it provides the basis for adjusting the plan when new opportunities and challenges present during or after the implementation (Friedman, 2018).

An IGA solution typically affects managers regularly because of their role in it, and it also impacts almost every employee in the organisation. For this reason, Friedman (2018) believes training and communication, implementation and measures should be part of the roadmap in order to achieve success of an IGA solution. Friedman (2018) focuses mainly on the implementation of IGA solutions, the study followed Friedman (2018) as a guideline for this reason.

2.2.1 Training

Training refers to the systematic activities that are organised and intended to encourage employees to acquire knowledge, skills, and attitudes (Salas et al., 2012). Friedman (2018) stipulates that organisation using an IGA solution must have continuous training tailored at three levels: All employees, Managers, and Security and IT teams.

According to Salas et al. (2012), training must aim to change how employees behave and think so that they can acquire competencies that are needed for their jobs. Friedman (2018) further state that an IGA training should focus on how to use an IGA solution and it should emphasise why the use of an IGA solution and understanding the policies related to it are important for employees, managers, and IT and Security teams. For managers specifically, the training should also emphasise why it is paramount to understand why they are approving access requests and why they are making a specific decision on access reviews (Friedman, 2018).

2.2.2 Communication

Friedman (2018) believes that communication is paramount for organisations implementing or using an IGA solution. Developing communication plans is vital in

information systems, and to communicate effectively, the objectives, activities, expectations, user input, and progress must be communicated openly (Denolf et al., 2015). Friedman (2018) stipulates that communication initiatives should inform employees about things they should expect from an IGA solution, and communication can also serve as the means to promote IGA successes because he believes that communication increases the user acceptance of an IGA solution.

2.2.3 Measuring deliverables

Like most projects, it is essential to break a project into deliverables and measure if the implemented deliverables delivered the promised value. One of the critical measuring techniques when dealing with an IGA solution is soliciting feedback from employees and managers. Soliciting feedback about the implemented deliverables will give the project team and steering committee signals around any confusion and resistance. Whatever the feedback they receive from employees and managers, the project team can use the feedback to refine and improve the IGA solution, processes and procedures. (Friedman, 2018)

Strategic roadmaps should plan for the long-term and assign dedicated resources to manage and maintain ongoing deliverables and plans (Garcia & Bray, 1997). Furthermore, Friedman (2018) state that measuring of deliverables and reporting of the feedback to the project team and steering committee should be in an IGA strategic roadmap and dedicated technical resources should be assigned to deal each deliverable.

To conclude the IGA section, the author is cognizant that the ongoing management and maintenance of an IGA solution and its components should have a long-term plan that consists of various initiatives to ensure that users and managers can realise the value that IGA solutions promise. The promised value of an IGA solution is, in summary, maintaining the CIA triad of informational assets with minimal identity-related threats. Furthermore, if the organisation does not plan accordingly, measure new deliverables, and solicit regular feedback from users and managers about the IGA solution and its components, there might be some user resistance.

2.3 User Resistance

2.3.1 Definitions

Various authors, such as Markus (1983), Marakas and Homik (1996), Kim and Kankanhalli (2009), and Klaus and Blanton (2010), in the field of information systems and management, have discussed the concept of user resistance. Sakala (2019) defines user resistance in Information Systems as any behaviours that deviates from an ideal information system being implemented, which ultimately result in minimal use or non-use of the information system by intended users.

Markus (1983) postulates that some individuals resist a system because they feel that there will be a distribution of power within the organisation. Consequently, they feel that by accepting and using the system, they will lose their power.

Marakas and Homik (1996) describe resistance behaviour as a passive-aggressive reaction to the threats and discomfort that users associate with the system. Users react in a resistant manner to communicate their distress about the system, system flaws, and/or system design (Marakas & Homik, 1996). For example, users were provided with a test system to see how the system works, as a result they found the system to be complex and slow, moreover, to communicate their dissatisfaction of the complexity and slowness of the test system they totally rejected the system (Newman & Robey, 1992). Lapointe and Rivard (2005) classify user resistance as an individual's reaction to the perceived threats associated with the adoption or usage of information systems.

Klaus and Blanton (2010) define user resistance as the behavioural conduct to oppose new information systems execution or usage. According to Joshi (1991), resistance behaviour arises when individuals perceive a change as unfair or a cause of inequity. However, research by Laumer, Eckhardt, & Weitzel (2016) stipulates that resistance behaviour may also arise as a result of choice, that is, whether the new system or technology adoption is mandatory or not.

Erwin & Garman (2010) noted that resistance is a multi-dimensional phenomenon that consist of three qualities, 1) involves how users react when responding to the change, 2) what users think concerning the change, and 3) how they feel concerning the change.

Kim and Kankanhalli (2009) explains resistance behaviour in terms of switching costs between moving away from the current technology to new technology. According to

Kim and Kankanhalli (2009), users would rather maintain their current situation than to change because they are certain about their current situation.

Klaus and Blanton (2010) explain user resistance as behaviour resulting from breaching a psychological contract. A psychological contract breach occurs when there is a conflict between individual issues, system issues, organisational issues, and process issues (Rousseau, 1989). A psychological contract is a unilateral belief that exist due to an overt promise becoming explicit and verifiable over time (Rousseau, 1989). For example, Rousseau (1989) explained that an employee might believe that hard work always results in continued employment because it resulted in continued employment over the years. Therefore, if there is an unfavourable change in the contract, the individuals (employees) who have psychological contracts may resist the change (Burnes, 2015).

The user resistance definitions by authors in the management studies cover similar angles like the one in the Information Systems research, which, for example defines user resistance as "behaviours intended to prevent the implementation or use of a system or to prevent system designers from achieving their objectives" (Markus, 1983:433). Enns et al. (2003) agree with the definition by Markus (1983), and the authors posit that such behaviours are sometimes shown by users not doing the expected, sometimes by delaying the process, and by arguing against the implementation of a system. On the other hand, Bagayogo et al. (2013) recognise that not all resistance behaviours are detrimental to an organisation, and not all acceptance behaviours are beneficial to an organisation. Bagayogo et al. (2013) agree that resistance behaviours are ultimately intended to prevent the implementation or use of a system or prevent system designers from achieving their objectives.

2.3.2 Causes of resistance

In a study by Rumelt (1995), the author reports that user resistance happens during strategy formulation or implementation. Resistance at a strategy formulation stage means that user resistance occurs during the strategy planning stages; resistance at implementation stages means that users' resistance behaviour occurs during the execution stages (Ali et al., 2016; Rumelt, 1995). Rumelt (1995) divided resistance causes into five groups and called them 'The Five Frictions', Del Val and Fuentes

(2003) then extended onto a study by Rumelt (1995) and categorised the five groups into sources of resistance in the formulation and implementation stages.

Although the focus of the study is on the usage of the access review component of SailPoint IIQ, the causes of resistance at formulation and implementation are relevant to the study because the issues that were not addressed at the formulation and implementation stages of SailPoint IIQ at ABC Bank can be the very issues that cause resistance during the adoption and use stage, which according to the adopted model is referred to as initial conditions, which will be discussed in detail under the theory section when discussing the model.

Table 1: Underlying causes of user resistance (Del Val & Fuentes, 2003:150)

Main sources of resistance	**Underlying causes of user resistance**
Resistance at the formulation stage	
i. Distorted Perception	Myopia Denial Perpetuation of ideas Implicit assumptions Communication barriers Organisational silence
ii. Low Motivation	Direct costs of change Cross subsidy comforts Cannibalisation costs Past failures Different interests among employees and management
iii. Lack of Creative Response	Fast and complex environmental changes Reactive mindset

Main sources of resistance	Underlying causes of user resistance
	Inadequate strategic vision
Resistance at the implementation stage	
i. Political and Cultural Deadlocks	Implementation climate and relation between change values and organisational values Departmental politics Incommensurable beliefs Deep-rooted values
ii. Other Sources	Leadership inaction Embedded routines Collective action problems Capabilities gap Cynicism

2.3.2.1 Resistance in the formulation stage

Resistance is not just an issue that occurs during implementation; it can happen during the formulation of a project in the strategy formulation (Del Val & Fuentes, 2003). As depicted in Table 1, resistance in the formulation stage consists of distorted perception, low motivation, and lack of creative response (Del Val & Fuentes, 2003).

2.3.2.1.1 Distorted perception

Del Val and Fuentes (2003) state that the first primary source of resistance in the formulation stage is distorted perception. Perception is the root of any change, and if there is distortion in the perception, the change results may be less favourable (Rumelt, 1995). The underlying causes of distorted perception are as per Table 1. According to Ali et al. (2016), distorted perception underlying causes observable in information systems are myopia, denial, and perpetuation of ideas.

Myopia

Myopia is the inability of an organisation to view the future of the business with a clear picture (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). Myopia can negatively affect an organisation (Smith et al., 2010), and individual myopia may lead to organisational inertia (Rumelt, 1995). In information systems, this could result in user resistance to information systems (Ali et al., 2016).

Denial

Denial is the refusal to acknowledge the information perceived as unfavourable (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). In social work research, denial is when users (such as alcoholics) refuse to accept the severity of their problem, which has led to individuals resisting the need for change (Watson, 2011). When individuals are in denial regarding the need for change in information systems, resistance may occur (Ali et al., 2016).

Perpetuation of ideas

The perpetuation of ideas is pursuing current thoughts regardless of the change in the circumstances (Ali et al., 2016; Del Val & Fuentes, 2003). The perpetuation of ideas can cause resistance to an information system because the users are comfortable with their current system and become uncomfortable with a new system or its ideas (Landaeta et al., 2008).

Implicit assumptions

These assumptions do not get discussed because of their inherent nature (Del Val & Fuentes, 2003); in information systems research, these assumptions are difficult to observe because of their nature (Landaeta et al., 2008).

Communication barriers

Communication barriers refer to any interference that can lead the communicating parties to misunderstand each other (Bredmar, 2017). Communication barriers can result in information distortion (Del Val & Fuentes, 2003), ultimately leading to resistance. However, in a study by Landaeta et al. (2008), communication barriers were not an evident source of resistance in the formulation stage.

Organisational silence

Organisational silence is a notion of individuals not expressing their thoughts in the formulation stage, which result in decisions taken with limited information (Del Val & Fuentes, 2003). Individuals being fearful of top management and being insecure of themselves are reasons for organisational silence (Beigi, 2015). Organisational silence can lead to resistance because the individuals might withhold the information critical for their adoption; as a result, meeting their unsaid expectations becomes challenging and might lead to them being resistant to the change initiative in later stages.

2.3.2.1.2 Low motivation

The second primary source of resistance in the formulation stage is low motivation (Ali et al., 2016; Del Val & Fuentes, 2003). Rumelt (1995) refers to low motivation as dulled motivation. Low motivation has five underlying sources, as listed in Table 1. The low motivation underlying causes observable in information systems are direct costs of change, cannibalisation costs, past failures, and different interests among employees and management (Ali et al., 2016).

Direct costs of change

The direct costs of change refer to the notion that a change can result in organisational failure, meaning that there might be disruptions in daily operations temporarily or permanently and that the change efforts can be expensive (Rumelt, 1995). Landaeta et al. (2008) suggest that users view these costs compared to the benefits of the change, and when the users perceive the costs to be high, there is a likelihood of resistant behaviour.

Cross subsidy comforts

These are the comforts resulting from the need to change a business compensated by the subsidies obtained without changes in another organisational unit (Del Val & Fuentes, 2003; Landaeta et al., 2008; Rumelt, 1995). Rumelt (1995) states that the subsidies could be direct or indirect, with direct subsidies being the management tolerance for losses paid off or balanced by the increases in other organisational units. The indirect subsidies are the subsidies by bundling the organisational units together so that all the business measures are treated as a whole and not isolated (Rumelt, 1995). Users may resist changes of this nature because there is no real motivation for the change to happen.

Cannibalisation costs

When change initiatives bring about the positives to the project, but their resultant factors are negative on another part of an organisation, such change initiatives require sacrifices within the organisation, changes of this nature are said to have cannibalisation costs (Ali et al., 2016; Del Val & Fuentes, 2003; Landaeta et al., 2008; Rumelt, 1995). Some organisations and individuals will resist a change of this nature because of the sacrifices they need to make.

Past failures

The failures of the past projects within an organisation leave the organisation's employees pessimistic about future projects (Ali et al., 2016; Del Val & Fuentes, 2003). When individuals are pessimistic about the projects, it might cause them to resist changes due to their past experiences.

Different interests among employees and management

When there are different interests between management and the employees, there tend to be cases whereby some employees do not value the change results as the management does (Del Val & Fuentes, 2003; Waddell & Sohal, 1998). In such cases, the employees that value the change results less are likely to be resistant to the change, and vice versa to those that value the change results.

2.3.2.1.3 Lack of creative response

The third primary source of resistance in the formulation stage is the lack of creative response (Ali et al., 2016; Del Val & Fuentes, 2003). Rumelt (1995) refer to it as a failed creative response. Table 1 depicts the three fundamental reasons that diminish creativeness when choosing change strategies. The lack of creative responses observable in information systems is fast and complex environmental changes, reactive mindset, and inadequate strategic vision (Ali et al., 2016).

Fast and complex environmental changes

When a change is happening faster, there tends to be limited time to perform an adequate situational assessment and analysis (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). The same limitation happens when the change is complex (Rumelt, 1995). Without proper situational analysis, organisations introduce changes because their competitors introduce them (Rumelt, 1995). Therefore, individuals within

that organisation might resist the change because of the different contexts within organisations. According to Landaeta et al. (2008), this is hardly observable where there is little turbulence.

Reactive mindset

When individuals and organisations believe that obstacles are natural and inevitable, Ali et al., (2016); Del Val & Fuentes, (2003); Rumelt, (1995), Landaeta et al. (2008), had observed that most personnel are used to the way they work and did not want to change. When change implementers observe obstacles and a change initiative continues without measures to eliminate the obstacles, the individuals who perceive an obstacle are likely to resist the change initiative.

Inadequate strategic vision

Creativeness diminishes when there is a lack of strategic direction, clear commitment, or support from senior management (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). When there is an inadequate strategic vision, some individuals resist the change initiative because they do not see its importance.

2.3.2.2 Resistance in the implementation stage

Implementation is an integral part of a change initiative, and it is a step where an organisation decides to change and adopt an information system (Rumelt, 1995). Del Val and Fuentes (2003) further stated that in the implementation phase, more resistance is observable than in the formulation stage.

2.3.2.2.1 Political and Cultural Deadlocks

The first primary source of resistance in the implementation stage is political and cultural deadlocks (Del Val & Fuentes, 2003). Rumelt (1995) refers to it as political deadlock. Table 1 depicts the four fundamental causes of resistance, and all four can be observed in information systems change initiatives (Ali et al., 2016).

Implementation climate and relation between change values and organisational values

Implementation climate refers to examining the implementation period with the values of a change initiative and an organisation (Del Val & Fuentes, 2003). If there is a negative gap between the values and the implementation climate, the change will likely

be opposed and resisted by the individuals (Ali et al., 2016; Del Val & Fuentes, 2003). Landaeta et al. (2008) did not observe this source of resistance because the organisational values and those of a change aligned.

Departmental politics

When the individuals within a department or managers of a department do not benefit from the change initiative or if they will suffer as a result of a change, this source of resistance is observable (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). Landaeta et al. (2008) observed this resistance where the nurses resisted the system implementation because the implementation implied extra responsibilities.

Incommensurable beliefs

This source of resistance is observed when the individuals or groups have strong but opposing beliefs about the change initiative (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). Landaeta et al. (2008) observed Incommensurable beliefs when two groups were accusing each other of the time taken to provide patients with transportation when patients get discharged, and both groups were sincere about their beliefs of who causes the delays.

Deep-rooted values

These are the values vested within an individual or group, and they develop some emotional loyalty (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). These values make individuals or groups have a sense of attachment to working (Rumelt, 1995). Users might become resistant if there is a change on something they are attached to or a change initiative affects them (Rumelt, 1995). Nurses and doctors may resist implementing an information system because they perceive a reduction in physical patient care they value (Landaeta et al., 2008).

2.3.2.2.2 Other sources

The second and last primary source of resistance in the implementation stage is other sources (Del Val & Fuentes, 2003). Rumelt (1995) refers to other sources as action disconnects. It has been referred to as other sources because it combines the sources of resistance of different nature and characteristics (Del Val & Fuentes, 2003). It consists of five fundamental causes of resistance, as depicted in Table 1. Ali et al.

(2016) acknowledged that all five fundamental resistance causes are observable in information systems.

Leadership inaction

Leadership inaction is a notion of senior management not taking any action to articulate a strategic vision for the change and directing change initiatives due to them fearing the unknown or having uncertainty about the change outcomes (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). Sometimes senior management does not take any action regarding change initiatives because they fear changing the status quo (Ali et al., 2016; Del Val & Fuentes, 2003; Landaeta et al., 2008). The lack of senior management support often increases employees' resistance to change (Kim & Kankanhalli, 2009).

Embedded routines

The way an organisation operates relies on processes, and over time, the organisational processes become more complex (Rumelt, 1995). As the organisational processes become complex, its processes operate tacitly than explicitly (Landaeta et al., 2008). When processes get more tacit, they become more complicated, and the complicated processes inherently possess high levels of resistance by users (Rumelt, 1995). Introducing changes to complex processes may be resisted because it may have many unintended consequences. After all, no one in the organisation understands the entire process due to its tacit nature.

Collective action problems

Collective action problems are the problems that happen because senior management does not coordinate the change initiatives, and individuals do not work together to realise the objectives of the change (Landaeta et al., 2008). The issues typically have to do with the individuals' lack of decisiveness to adopt the change first (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). A study by Landaeta et al. (2008) observed this resistance when there was no coordination of the change initiative by senior management.

Capabilities gap

Capabilities gap refers to the gap between the change initiative that needs implementation and the capabilities and competencies needed to implement a change

initiative (Rumelt, 1995). When the required capabilities and competencies are lacking within an organisation, the users will likely resist a change initiative (Ali et al., 2016; Del Val & Fuentes, 2003; Rumelt, 1995). Landaeta et al. (2008) did not observe this resistance because senior management support ensured that individuals within the organisation are well equipped to deal with the change.

Cynicism

Cynicism is the notion of individuals being sceptical about the success of the changes (Del Val & Fuentes, 2003; Landaeta et al., 2008; Selander & Henfridsson, 2012). Selander & Henfridsson (2012) stipulates that when individuals are sceptical about the success of a change, it is likely to influence them to be resistant to a change initiative. Landaeta et al. (2008) observed cynicism when nurses started to be doubtful about the success of the change due to the way doctors were responding; this is because the doctors' discharge information was a significant contribution to the system's functions. However, the doctors were 'very' busy for them to provide such information.

2.3.2.3 General Causes of Resistance

A study by Seo et al. (2011) stipulates that some individuals are resistant to change because they perceive that a system does not complement the organisational routines. Some employees resist change because they are uncertain of the consequences of using the system, and others resist change because they fear losing autonomy (Seo et al., 2011).

2.4 Resistance Behaviour

The primary dimension for resistance is behaviour (Lapointe & Rivard, 2005) . Various authors Coetsee (1993); Hirschheim and Newman (1988); Lapointe and Rivard (2005); Rivard and Lapointe (2012); and Senn (1978) acknowledge that resistance behaviour varies in different settings.

Apathy is a stage in which the user is indifferent about the system or show a lack of interest in the system (Coetsee, 1993). Passive resistance is a stage in which the user is starting to show the intent to resist the system, and symptoms include excuses and persistent lack of interest (Coetsee, 1993). Active resistance is a stage in which the user makes it visible that they do not want to use a system; its indicators include voicing out negative opinions about the system and forming groups against the system

(Coetsee, 1993). Aggressive resistance is a stage in which individuals try to disrupt the use of the system through actions such as threatening other employees and striking (Coetsee, 1993).

Coetsee (1993) defined resistance behaviours are similar to those defined by Senn (1978). Projection and passive resistance are like resistance behaviours as compared to each other. Furthermore, avoidance and passive resistance are similar.

2.4.1 General Resistance Behaviour

Organisations implement new information systems to be innovative and continuously improve their productivity (Adeleke, 2016; Burnes, 2015). However, implementing new systems does not always result in successful use and adoption (Adeleke, 2016; Burnes, 2015). User resistance behaviour does not always equate to the refusal to use the system. Seo et al (2011) categorised user resistance into two groups, which includes the group where users are resistant to a change but use the system regularly, and one where individuals do not use the system at all or use it minimally.

Ford and Ford (2009) stipulated how user resistance to a change can benefit the change process. User resistance can benefit a change process by boosting awareness to the individuals that enquire about the change, the answers that change implementers provide build the awareness of what the change entails (Ford & Ford, 2009). While user resistance boosts awareness, it also helps the change implementers explain the purpose and importance of the change, which ultimately gets more individuals' participation (Ford & Ford, 2009).

When more parties are involved and can explain their reasons for resistance, it gives the change implementers the ideas of the aspects they did not consider at the beginning of the change initiative. As a result, the change goes forward with some amendments to cater to the individuals' needs (Ford & Ford, 2009). Some individuals resist change due to experience from the previous change initiatives in the organisation (Ali et al., 2016; Del Val & Fuentes, 2003; Ford & Ford, 2009). The change implementers can use previous experiences as input to not repeat the same mistakes by previous implementers (Ford & Ford, 2009).

2.5 Theoretical Background

Studies have used various models, frameworks, and theories in information systems research to explain user resistance to information systems. Some of the models and

frameworks include The Political Perspective by Markus (1983), Passive Resistance Misuse by Marakas and Homik (1996), and Multilevel Model of Resistance to Information Technology Implementation (Lapointe & Rivard, 2005).

2.5.1 The Political Perspective

Markus (1983) describe resistance by means of the interaction between the system and the context in which the system is used. Markus (1983) postulate that users that believe that a system will support their position of power in the organisation are inclined to use and support the system. However, if the users believe that the system will result in the distribution or loss of power, they will resist the system. Moreover, The Political Perspective model depict resistance as a consequence of interaction between the features of a system with the intra-organisational distribution of power (Markus, 1983). In addition, Markus (1983) suggests that the severity of resistance is directly affected by the size of the power distribution together with its perceived importance.

Markus (1983) noted that the political perspective is more applicable to the systems that are used across the organisation. The Political Perspective model by Markus (1983) was not adopted for the study because it mainly focuses on the political and power dimensions of user resistance to the information system. The other reason that the study did not adopt the model is that the study does not wish to devise strategies to deal with resistance, nor does the study wish to design a system. The study aim was to examine why some bank managers do not use the access review component of SailPoint IIQ. Using the framework by Markus (1983) would narrow the study to examining factors related to power and politics, and there might be more or other reasons why some bank managers do not use the access review component of SailPoint IIQ. The study wished to capture reasons other than those related to power and politics. Therefore, this framework was not the most suitable one for the study.

2.5.2 Passive Resistance Misuse

Marakas and Homik (1996) postulate that resistance behaviours are reactions to threats that individuals relate with a new system, with the nature of the reactions being passive-aggression. Passive resistance misuse is the uncooperative, hidden behaviour resulting from fear and anxiety from introducing a new system into an environment that the user deems stable (Marakas & Homik, 1996). Additionally, Marakas and Homik (1996) focused on user resistance that personal interest or

criminality has no influence over; they focus on the behaviours that can be confused as users accepting and are cooperative with the new system. However, these behaviours have hidden resistance that might also consist of efforts to sabotage the implementation of the system.

Marakas and Homik (1996) model was not adopted for the study because it mainly focuses on hidden user resistance to the information system. While the model is helpful in the user resistance literature, the study aim was to examine why some bank managers do not use the access review component of SailPoint IIQ, which includes all kinds of resistance behaviours, hidden and explicit. Using the framework by Marakas & Homik (1996) would narrow the study to examining factors related to the hidden resistance of managers using the access review component of SailPoint IIQ. The study also wished to capture reasons other than managers using the access review component of SailPoint IIQ with hidden resistance. Therefore, this framework was not the most suitable one for the study.

2.5.3 A multilevel model of resistance to information technology implementation

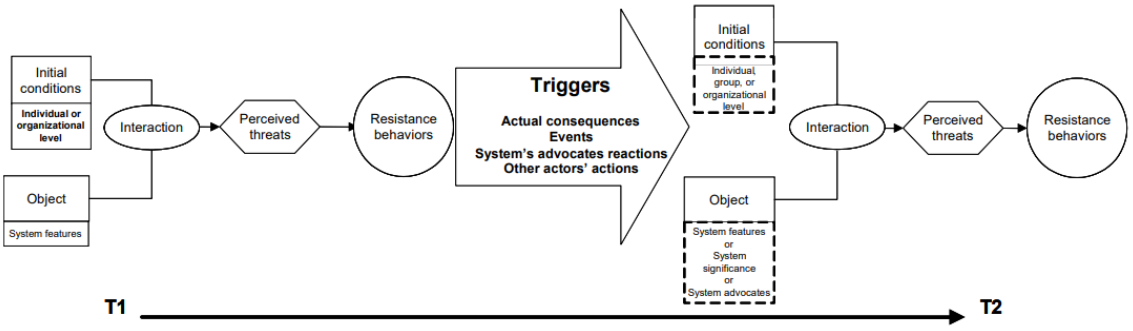


Figure 1: Resistance to IT Implementation: A Longitudinal Perspective (Lapointe & Rivard, 2005:480)

Figure 1 depicts a model Lapointe and Rivard (2005) proposed for explaining user resistance behaviour; it posits that user resistance happens because of perceived threats. This is the model that this study adopted.

Lapointe and Rivard (2005) conducted a longitudinal study and developed their model by first assessing the existing models of resistance to information systems. The model that they assessed were developed by Joshi (1991), Marakas and Hornik (1996), Markus (1983), and Martinko et al. (1996). Thereafter, to develop the theoretical phenomenon and their underlying concepts, Lapointe and Rivard (2005) performed a

semantic analysis, and the result was five common components namely, resistance behaviours, object of resistance, perceived threats, initial conditions, and subject of resistance.

‘Resistance behaviour’ refers to how the individual reacts when resisting, and an ‘Object of resistance’ can either be a system’s feature, system’s significance, or system’s advocates (Lapointe & Rivard, 2005; Sakala, 2019; Selander & Henfridsson, 2012). ‘Initial conditions’ refers to the individuals’ or group’s subjectivities that influence how an object is perceived, and perceived threat is a consequence of the interplay between the initial conditions and the object of resistance that the subject of resistance utilises (Lapointe & Rivard, 2005; Sakala, 2019; Selander & Henfridsson, 2012). A ‘subject of resistance’ refers to an individual or group that exerts a resistance behaviour (Lapointe & Rivard, 2005; Sakala, 2019; Selander & Henfridsson, 2012). ‘Interaction’ is a concept that exist when there is an Object of Resistance and Initial Conditions, therefore the study did not explicitly discuss interaction as a concept..

Lapointe and Rivard (2005) further examined the existing models to understand the relationships that exists between the identified components, and to improve their interpretation of the multilevel nature of the phenomenon.

Analytic induction was used to examine the data that was collected from three the case studies for information systems implementations in hospital settings (Lapointe & Rivard, 2005). The results of the analysis revealed that when there are mixed determinants, the nature and intensity of resistance varies between (Lapointe & Rivard, 2005):

- Individuals or groups being indifferent about using the system
- showing their lack of interest in using the system,
- complaining about a system
- resisting actively by forming coalitions
- behaving aggressively by threatening to resign, causing troubles and rebelling

According to Lapointe & Rivard (2005) model as depicted in Figure 1, users first assess a system based on the interplay between its features and initial conditions and then project the consequences of using it. Moreover, if they project a system to have threatening consequences, they will behave in a resistant manner. They argue that

conducting a study using their model allows the researcher to examine the consequences of using the system and highlight the ‘triggers’ that can change ‘initial conditions’ or ‘object of resistance’. “Triggers include consequences of system use, other actors’ actions, system advocates’ reactions to resistance behaviors, and events related to the implementation process” (Lapointe & Rivard, 2005:479).

Lapointe and Rivard (2005) also reviewed the literature in psychology, political science, sociology, and change management to better define and explain resistance behaviour. However, the model adopted the user resistance taxonomy by Coetsee (1993). Coetsee (1993) outlines four resistance levels in the taxonomy: apathy, passive resistance, active resistance, and aggressive resistance.

2.6 Conceptual Framework

Figure 2 represents the conceptual framework that the study adapts from Lapointe and Rivard (2005). The study uses the framework to explain the resistance behaviour that managers possess at ABC Bank.

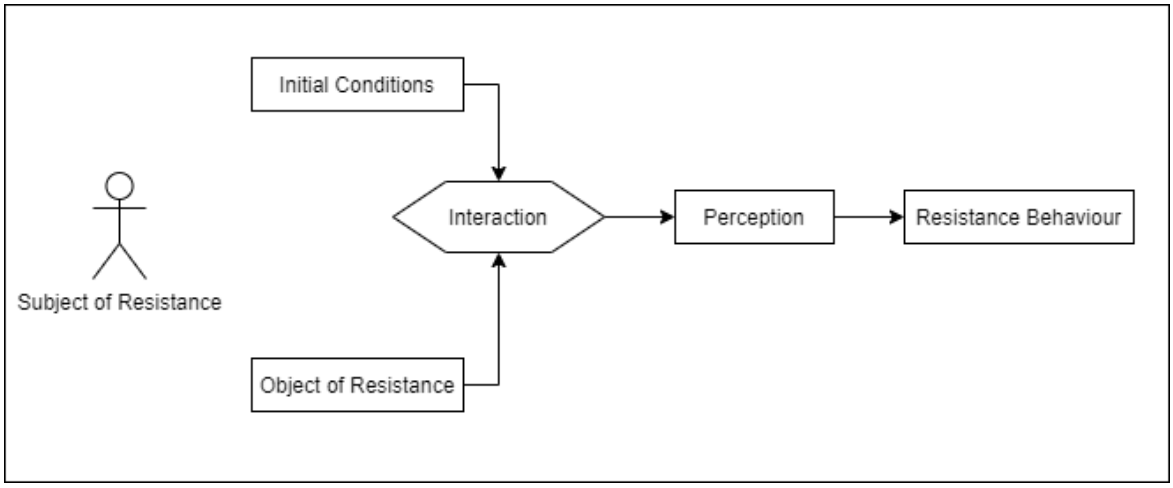


Figure 2: Conceptual Framework

2.6.1 Resistance behaviour

User resistance is multi-disciplinary, and the factors that impact and influence user resistance are similar in various areas such as information technology, information systems, human resources, and organisational behaviour (Ali et al., 2016). Therefore, the study also considers factors from disciplines outside of information systems.

The resistance behaviour concept enabled the study to answer the secondary research question, “How do bank managers behave towards the access review component of SailPoint IIQ?”

2.6.2 Object of resistance

According to Selander and Henfridsson (2012), an object of resistance is the content that users resist. When studying resistance, it is vital to identify and understand the content that the target audience is resisting (Selander & Henfridsson, 2012). In the field of information systems, Joshi (1991) points out that individuals or target audiences resist implementing or using a system they perceive will have unfavourable results towards them or the organisation. Lapointe & Rivard (2005) recognise the object of resistance as the system itself, system significance, and system advocates.

The system itself denotes the specific features within the system, and the users tend to resist the features that do not meet their expectations (Lapointe & Rivard, 2005; Sakala, 2019; Selander & Henfridsson, 2012).

‘System significance’ posits that individuals resist a system because of the meaning they put in adopting the system. Some individuals reveal some resistance towards a system when they see that it is highly likely to change the status quo or power structures (Lapointe & Rivard, 2005; Sakala, 2019; Selander & Henfridsson, 2012).

‘System advocates’ posits that individuals do not resist the system itself or its significance, but they resist the entire system’s implementation process based on who is at the forefront of the system implementation (Lapointe & Rivard, 2005; Sakala, 2019; Selander & Henfridsson, 2012).

The study defines an object of resistance as the system, the component of the system, system advocates, system significance, and processes that managers are resisting.

The system that managers resist is SailPoint IIQ, and the component of the system is the access review component of SailPoint IIQ. Furthermore, the system significance is the importance and rationale for having a SailPoint IIQ and performing the access review exercise on SailPoint IIQ. The System advocates are the custodians of SailPoint IIQ at ABC Bank, including the Division itself and management responsible or accountable for supporting SailPoint IIQ.

One of the managers responses in Selander and Henfridsson (2012) highlighted that some users resist a system because of the complex processes that the system introduces.

> *"How do you communicate [to members of the staff] that 'well we bought this new system that will make every work process more complex and time consuming than before. To compensate, we will need to increase our workforce with 200% during the next one and a half year– how do you feel about that?"* (Selander & Henfridsson, 2012:305)

According to the participants' responses in Selander and Henfridsson (2012), due to the complex processes that the system introduced, their turnaround time of Twenty-Four (24) Hours is impossible to meet because the new system takes them around two months to respond to clients.

> *"I have answered incoming customer emails since October. When I started working on this, we were expected to answer within 24 hours, yet today [with the new system] it takes about two months to provide an answer."* (Selander & Henfridsson, 2012:305)

'Process' is defined in this study as the activities involved in performing an access review.

The object of resistance enabled the study to answer the secondary research question, "What do bank managers resist?"

2.6.3 Initial conditions

Lapointe and Rivard (2005) postulate that 'initial conditions' introduce individuals' or groups' subjectivities that influence the extent of the threat that individuals perceive. For example:

- The established power and political structures within an organisation as stated by Markus (1983) can influence how individuals perceive a threat of distribution of power as a result of adopting or using a system.
- Work routines and organisational structures as stated by Kim and Kankanhalli (2009) can influence how individuals perceive a threat of disturbing the status quo if a system is adopted or used within the organisation.

- The already existing inputs and outputs as stated by Joshi (1991) can influence how individuals perceive a threat. Users might believe that by adopting and using a system, there might be additional inputs expected from their side such as learning how to use a system (Joshi, 1991). The users might also perceive the negative outcomes of using a system to be something like losing a bargaining power and losing an opportunity to advance their careers (Joshi, 1991). Therefore, the use of a system might disturb the already existing inputs and outputs if the gains that the users will get from the use of the system is not apparent (Joshi, 1991).

Some authors studies the causes of resistance (Ali et al., 2016; Del Val & Fuentes, 2003, Rumelt, 1995), this study looks at the causes of resistance as 'initial conditions' because there is resistance that is already existing.

2.6.4 Perceived threat

The perceived threat is the negative consequence that a user or potential user predicts (Lapointe & Rivard, 2005; Selander & Henfridsson, 2012). A neuroscience study by Fernandes et al. (2013) stipulates that individuals' defensive behaviour under certain circumstances is determined by whether the individuals perceives a threat or not. Several authors such as Dent and Goldberg (1999); Fugate et al. (2010); Joshi (1991); and van Dijk and van Dick (2009) acknowledge that resistance behaviour is a reaction that arises as a result of a user perceiving negative consequences that a change initiative brings.

The study focus is the perception and not just the negative perception that the managers might have towards the object of resistance. The study adapts perceived threat to a perception that managers have towards the object of resistance.

2.6.4.1 The rationale for 'perception' instead of 'perceived threats'

Most of the studies in Information Systems study perception, "Perception is man's primary form of cognitive contact with the world around him. As all conceptual knowledge is based upon or derived from this primary form of awareness" (Efron, 1969). This study seeks to study perception in its entirety than just the 'threat' perception. Studying the resistance behaviours from a perception point of view instead of perceived threats will broaden the scope of other studying resistance behaviour.

‘Perception’ will allow the researcher to study other concepts that are not necessarily threats, however, such concepts were previously studied by researchers such as Davis (1989) and Rogers (1995) to influence use and adoption of users.

While this study does not adopt the technology acceptance theories as adopted by Sabi et al. (2015), the independent variables from the Technology Acceptance Model and Diffusion of Innovation theory will help understand the behaviour of managers in ABC Bank. Perceived usefulness and perceived ease are the independent variables of the Technology Acceptance Model (Davis, 1989).

Davis (1989) refers to the ‘perceived usefulness’ as the degree to which individuals believe that using a specific technology would improve their job performance. ‘Perceived usefulness’ is similar to the compatibility of technology as stipulated by Bradford and Florin (2003) and Rogers (1995), as it implicitly looks at how the use of specific technology complements the job that an individual does. While ‘perceived usefulness’ is not a threat, its lack could lead users to resist a technology (Bradford & Florin, 2003; Davis, 1989; Rogers, 1995).

Davis (1989) refers to ‘perceived ease of use’ as the degree to which individuals believe using a specific technology would require less effort. ‘Perceived ease of use’ is similar to technology complexity as stipulated by Bradford and Florin (2003) and Rogers (1995) because it looks at the effort that individuals perceive as required to use the specific technology. While ‘Perceived ease of use’ is not a threat, its lack could lead users to resist a technology (Bradford & Florin, 2003; Davis, 1989; Rogers, 1995).

Other perceptions can influence users’ decisions to use technology (Charness & Boot, 2015). Moody et al. (2018) studies the role of punishing individuals for not complying with information security policy, and the study concludes that punishing individuals does not necessarily influence users to comply with the policy. However, some respondents in Moody et al. (2018) exhibit that punishment influences them to comply with the policy. This study will also inquire whether some managers do not perform access reviews on SailPoint IIQ because there is a ‘lack of perceive consequences’ to them for not performing access reviews through SailPoint IIQ.

2.6.5 Subject of resistance

The subject of resistance is an individual, group, or organisation that adopts the resistance behaviour (Lapointe & Rivard, 2005). The study defines the subject of

resistance as individuals that possess the resistance behaviour towards the Access Review component of SailPoint IIQ within ABC Bank. According to the study, these are all the levels of management from middle management, senior management, to executive management.

CHAPTER 3: *RESEARCH DESIGN AND METHODOLOGY*

The objective of this section is to describe the research design and methodology that the study uses. It will start by describing the research paradigm that the study adopts, and then provide a detailed description of the research design that the study uses to collect and analyse the data.

3.1 Research Paradigm

Research is a process of gathering information to generate new knowledge (Oates, 2006). Bhattacherjee (2012) defines scientific research as a systematic inquiry into a natural setting to discover laws and suggest theories to describe social phenomena. Proper academic research uses a research paradigm or research philosophy that demonstrates how the researcher will reason and observe the natural setting and how the researcher can attain knowledge about the natural setting (Oates, 2006). A research philosophy or paradigm is a collection of shared assumptions about reality (Bloomberg et al., 2011; Oates, 2006). There are two main research paradigms in information systems research, namely interpretivist and positivist (Bloomberg et al., 2011; Oates, 2006). This study favours the use of an interpretivist paradigm to study the reasons why bank managers resist the use of the access certification component of SailPoint IIQ.

3.1.1 Interpretive research paradigm

An interpretive research views the social world in its context; individuals' realities and interpretations of the world are subjective based on their social setting (Bhattacherjee, 2012; Bloomberg et al., 2011; Oates, 2006). In information systems, an interpretive study identifies, explores, and explains how factors are related and interdependent by looking at how the individuals perceive the world in a social context within which the system resides (Oates, 2006). People assign subjective meanings and values to a phenomenon under observation (Bhattacherjee, 2012). Understanding people's meanings and values provides a rich understanding of a specific context, and observations can be drawn specifically for that context (Myers, 1997; Oates, 2006; Orlikowski & Baroudi, 1991).

The study adopts the interpretive paradigm following an inductive approach because of the nature of the study. Within the broader scope of interpretive paradigm, this study employs a qualitative research method because its aim is not to generalise the

research findings to a population. Qualitative research interprets an observed phenomenon concerning the subjective meanings that individuals give to the phenomenon (Bloomberg et al., 2011; Hunter, 2005; Oates, 2006). This study aims to understand the managers' perception of why some managers do not use the access review component of IIQ.

The qualitative research method uses qualitative data such as interviews, observation results, and documents (Myers, 1997). Interpretivist research typically employs an inductive approach, and it aims to categorise the gathered data to develop or build upon a theory relating to the phenomenon (Oates, 2006; Orlikowski & Baroudi, 1991).

In contrast to the interpretive paradigm is the positivist paradigm. The positivist research paradigm aims to test theory; it seeks to generalise observations (Oates, 2006). Positivist research assumes that the absolute truth is attained by gathering objective facts, and the social world can be reduced into simple elements that can represent its truth (Bloomberg et al., 2011). The positivist paradigm fails to recognise the individuals' subjective meanings and interpretations of a social world, and it is mainly suited for natural sciences research (Oates, 2006). Information systems primarily draw from social sciences research (Hunter, 2005); it is for this reason why the researcher did not employ the positivist paradigm to study managers' perceptions.

The nature of the study is to address the 'what', 'how', and the 'why' questions. Multiple research designs and strategies can fulfil a study following an interpretive paradigm (Bloomberg et al., 2011). The following section discusses the research design and strategy.

3.2 Research Design and Strategy

A research design constitutes a plan and structure that an author will use to realise the research objectives and answer the research questions (Bloomberg et al., 2011). Research design includes the data collection process, research instrument, and sampling process that the study will employ (Bhattacherjee, 2012).

Within the broader interpretative paradigm, this study follows an explanatory research design. An explanatory study explains the rationale of an observed phenomenon; it goes beyond descriptive studies and explains why an event occurs (Bloomberg et al., 2011; Oates, 2006). An explanatory study can be said to address the 'why' of research. This study aims to explain why some bank managers do not use the access review

component of SailPoint IIQ, which makes explanatory design a research design of choice. The other research designs that the study can follow to conduct academic interpretive research are exploratory and descriptive (Yin, 2003).

The study aims to explain user resistance in the context of a South African Bank and explain why some bank managers do not use the access review component of SailPoint IIQ. The study accomplishes this by exploring the circumstances that influence managers not to use the access review component of SailPoint IIQ and uncovering what managers resist. The study was able to expose the managers' behaviour towards the access review component. Thereafter, the study explains why there is such behaviour.

The study can use various strategies to conduct an explanatory study (Yin, 2003). The strategies also depend on whether the study takes an inductive or deductive approach (Saunders et al., 2009a). The study follows an inductive approach. Therefore, a case study strategy was adopted to enable researchers to study a phenomenon in a real-life context (Yin, 2003).

3.2.1 Case Study Strategy

A case study research strategy for conducting research is an empirical inquiry that involves examining a phenomenon within its real-life context (Robson, 2002; Yin, 2003). With a case study, the boundaries between the phenomena under investigation and the context of the phenomena are not clear (Yin, 2003). A case study strategy is appropriate when the researcher wishes to thoroughly understand the context when studying a phenomenon (Morris & Wood, 1991). A case study strategy is common for studies that adopt explanatory or exploratory research design because of its ability to answer the 'what', 'how', and 'why' research questions (Saunders et al., 2009a). Furthermore, the insights gained from using a case study strategy help develop new descriptions and theoretical outlooks (Bloomberg et al., 2011). In information systems, the case study strategy has been successful, and for qualitative explanatory research, it is the recommended tool (Myers, 1997; Walsham, 2017).

A case study strategy is typically executed in an interpretative manner and relies primarily on qualitative data to understand the phenomenon's real-life context (Yin, 1994). The case study strategy enabled the study to establish the factors that influence bank managers not to use the access review component and examined what

managers are resisting, and thereby examined the managers' resistance behaviours. The study's research questions can only be answered by understanding the context under which the bank managers are resisting or not using the access review component.

Information Technology and the business environment change quickly (Xia & Lee, 2005). The continuous changes results in many topics emerging every year, of which significant insights can be sought using case research (Benbasat et al., 1987). According to Benbasat et al. (1987), the case study strategy is viable for information systems research for the following reasons:

- It enables the researcher to study information systems in a natural setting. This study took place at one of the South African banks.
- The study can answer the 'how' and 'why' questions by the case study research. This study seeks to understand the 'why' question, that is, 'Why do bank managers resist the use of the access review component of SailPoint IIQ?'. T
- A case study strategy is well suited for areas where only a few studies have been carried out in information systems. Although there is much literature on user resistance in information system research, they have been carried out in different contexts, and few studies have considered a South African bank with an emphasis on the access review component of an IGA Solution.

3.3 Time Horizon

The study was conducted at one time-period. Therefore, this study employs a cross-sectional time horizon. A cross-sectional study is a study that is conducted at a single point in time (Bloomberg et al., 2011; Orlikowski & Baroudi, 1991). A longitudinal study is an alternative to cross-sectional; the longitudinal study was ruled out mainly because of the limited time allowed to complete a Masters research report; longitudinal studies require 'before and after' snapshots over a period, these studies often take years to complete (Bhattacherjee, 2012; Orlikowski & Baroudi, 1991).

3.4 Sampling

Sampling is a process whereby a subset of a population, sample frame, and a sample is selected in order to make an observation (Bhattacherjee, 2012). A population is a group of people that poses the characteristics that the researcher wishes to study

(Saunders et al., 2009b). The population for this study is all the managers that have been in ABC Bank employ for over twelve months.

Sampling managers that have been working for the Bank for at least twelve months is because they would have received an email to complete an access review for their subordinates. Moreover, the Bank also granted the researcher permission to only interview individuals that have been in the employ for over twelve months.

A sample frame is a section of the population that is accessible (Bhattacherjee, 2012). The sample frame of this research is all the bank managers under the ABC Bank employ in South Africa. The researcher is using managers in South Africa because they are all accessible through Microsoft Teams. A sample refers to the individuals that the researcher will select for observation (Bhattacherjee, 2012).

Qualitative research typically employs nonprobability sampling, and the commonly used sampling techniques are purposive sampling, snowball sampling, and convenience sampling (Cooper & Schindler, 2014).

Purposive sampling is a sampling technique that chooses a sample based on the participants' characteristics (Bloomberg et al., 2011). Purposive sampling is the sampling technique that the study employs because the researcher has permission to access the database that has potential participants within the bank.

3.5 Study participants (Sample)

The permission was granted for the researcher to conduct the study on employees that have been in the bank's employ for at least twelve months. Apart from the permission that was granted, the study had also chosen the managers who had been in ABC Bank's employ for at least twelve months because the access reviews typically occur at least once in a year at ABC Bank. Moreover, ABC Bank's information security policy suggests that access reviews must happen at least once a year for normal access and at least twice a year for privileged access. Therefore, within the twelve months of employment, the manager would have received a notification to perform an access review for the subordinates through SailPoint IIQ, and as a result these managers will be able to provide some rich and in-depth data towards the study.

The study wished to include the executive, senior, and middle managers as primary targets of the study. Table 2 is an indication of the targets for the interviews per level of management.

The study interviewed both male and female managers, managers of different age groups, managers from different teams/divisions, and managers of different ethnicities.

Table 2: Interview Targets per Management Level

Management Level	**Study Definition**	**Target for interviews**	**Total respondents**
Executive Management	Managers whom their subordinates are Senior managers and any level above senior management. These are typically Heads of Divisions, and C-Level Executives.	At least one manager from this level	3
Senior Management	Managers whom their subordinates are middle managers. These are typically Heads of departments.	At least three managers from this level	4
Middle Management	Managers whom their subordinates do not have subordinates according to the organisational structure. These are typically operational managers or line managers.	At least six managers from this level	4

3.6 Data Collection

Data collection is an integral part of research, and it is defined as a process of gathering information from target audiences with an aim to inform the study results (Polkinghorne, 2005). Qualitative data is typically the data collection technique employed by a case study (Myers, 1997; Yin, 1994). Qualitative data include field

observations, interviews (with open-ended questions), archive records (e.g. service records, budgets, and reports), documents (e.g. meeting minutes, agendas, and progress reports), and physical artefacts (Myers, 1997).

Literature played an influential role in the questions that make up the research instrument (Appendix A) and the 'Multilevel model of resistance to information technology implementation' framework by Lapointe & Rivard (2005). Following is how the framework influenced the interview questions:

Resistance behaviour concept refers to how users behave after perceiving a threat, the researcher developed a question to extract information about managers' resistance behaviour from participants, the question was:

> *How do you believe managers resist the access review component of SailPoint IIQ? Why?*

Perceived threat concept refers to how users perceive the interplay between the object of resistance and initial conditions, the researcher developed a question to extract information about managers' perceptions that might lead them to behave in a resistant manner, the question was:

> *What do you think are some managers' perceptions or views about the access review component of SailPoint IIQ that might lead them to not performing access reviews on it?*

Initial conditions concept refers to the individuals or groups subjectivities that can influence how the users perceive the object of resistance. Based on this, the researcher developed questions to extract information about managers' subjectivities that might influence them to behave in a resistant manner towards the object of resistance, the questions were:

> *What do you believe are the factors influencing managers not to perform access reviews on SailPoint IIQ?*

And an optional question which could was asked depending on how detailed and clear the previous question was asked, the optional question was:

> *Based on what you just said, what would you say makes the managers not to perform access reviews on SailPoint IIQ?*

Object of resistance concept refers to what the users can resist, the model suggest that users can resist the system itself, system significance, and system advocate. Based on this, the researcher developed a question to extract information about what the managers are resisting, the questions were:

What do you think bank managers are resisting?

The data that the study collected is qualitative data. The study employs the following procedures, methods, and sources when collecting data and ensuring that the data that will be collected is valid and reliable.

3.7 Interviews

The primary data collection method that this study employs is semi-structured interviews. The interviews were conducted electronically.

Semi-structured interviews involve the use of prepared questions, and an interviewer can change the order of the questions (Bloomberg et al., 2011). In qualitative research, semi-structured interviews are the commonly used technique for data collection (King, 2004). According to King (2004), the researcher can change the questions and omit some questions when conducting interviews if new information arises.

Semi-structured interviews are well applicable for cases where obtaining an in-depth understanding of a phenomenon is necessary and for cases where understanding the meaning individuals assign to a phenomenon is essential (Bloomberg et al., 2011).

During the interviews, where necessary, the researcher made use of some South African informal day-to-day language that is common in a business environment, for example, ‘oh ye?’, ‘you don’t say’, ‘is it?’, ‘hau’, ‘I see’, ‘I can imagine’, ‘I get you’,’hundreds’,’yeah’,’cool’,’alright’,’ayt’. The use of informal language was used as a probing technique for study participants to talk more.

Managers were asked for permission to audio-record the session at the beginning of the interview. However, a consent form was attached to the meeting invite, and accepting a meeting invite was deemed as providing consent to participate in the interview. In cases where managers did not accept the meeting but attended it, the researcher walked managers through a consent form, and they verbally provided consent.

A secondary plan to collect primary data if the electronic sessions did not work for the interviewee, the researcher's plan was to request consent from the participant to use the mobile number residing in the ABC Bank email client. If the manager agrees, a meeting invite would have been sent via email, and the researcher would call the manager at the respective time. Managers would have been asked for permission to audio-record the session at the beginning of the mobile voice call. However, there was no instance whereby the researcher had to execute a secondary plan.

3.8 Data Analysis

Data analysis is the process of reducing and assessing the data using methods that allow the researcher to present the data in a manner that is logical and usable (Hamon et al., 2003). The focus of data analysis for this study was to understand and explain why bank managers resist using the access review component of SailPoint IIQ. The analysis aimed to outline the context and the factors influencing bank managers to behave in a resistant manner towards an access review component of SailPoint IIQ.

Seidel (1998) describes the qualitative data analysis using and iterative model, which describes data analysis a process that iterates between noticing things, collecting things, and thinking about things.

The use of semi-structured interviews gave the researcher the flexibility for restructuring the questions and asking more or fewer questions as more information emerged during interviews. This technique provided the researcher with information that allowed for a thick and deep description of the research

Thematic analysis for qualitative research was the method of choice used to analyse data in this study. According to Braun and Clarke (2006), thematic analysis comprises of six phases, which are as follows:

1. Familiarising yourself with your data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing the report

The following section outlines how each of the phases were applied in the analysing the collected data. The phases defined by Braun and Clarke (2006) were employed to analyse the raw interview data obtained from the study participants which establishes rigour in the data analysis process.

After collecting data using interviews, the verbal data was transcribed into written form for the thematic analysis to be conducted. The transcription process offered the researcher a significant means to get more familiar with the data and start putting meaning to the collected data, identifying patterns, themes, and potential relationships. The researcher noted down the apparent themes that were coming up during the transcription process to reference them later.

The coding process to group ideas and themes started after the interview data was transcribed. Figure 3 depicts the *a priori* themes, the coding process began with the generation of initial codes to be used for the fundamental aspects of the conceptual framework on interview transcripts that the researcher printed for coding purposes. The fundamental aspects included subject of resistance, object of resistance, initial conditions, perception, and resistance behaviour.

Priori theme	Code	Description
Subject of resistance	SR	Subject of resistance refers to the individuals, groups, or organisations that adopts the resistance behaviour
Object of resistance	OR	Object of resistance refers to the objects that individuals, groups, and organisations are resisting.
Initial conditions	IC	Initial conditions refers to the subjectivities that managers possess at an individual level. It includes the already existing inputs and outputs, the established power and political structures, work routines, organisational structures, and individuals already existing perceptions and views about SailPoint IIQ and access reviews.
Perception	P	Perception refers to what managers think after their subjectivities inteacts with the object of resistance.
Resistance behaviour	RB	Resistance behaviour refers to how managers behave after developing a perception.

Figure 3: A Priori Themes

Moreover, additional coding was added on the printed interview transcript to further identify sub-themes. The sub-themes are mostly ‘data-driven’, meaning that the sub themes were mostly developed from the interview feedback (Braun & Clarke, 2006). Figure 4 highlights a sample of a sub-theme that was developed from the transcript data. The researcher code ‘OR-Proc’ was marking all responses that suggested that

managers are resisting the access review process as opposed to the system itself (OR-S), system significance (OR-SS), and system advocates (OR-SA). Figure 4 is not an entire list of sub themes that were developed through this process.

Transcript	Code
…they resist the process in its entirety, what do I mean by that? They resist having to spend a lot of time finding out what they are certifying, which is a very daunting process…	OR-Proc
…there was no easy way for him (Participant's Manager) to go through the process…	OR-Proc

Figure 4: Coding Sample

After the coding process was complete, the researcher transferred the codes to a spreadsheet which described the meaning of each code. Figure 5 provide a sample of descriptions of the codes.

Code	Description
IC-UA	Initial conditions that were due to unclear access, so be it because of lack of descriptions on the access, or use of a technical jorgon that managers do not understand
IC-PE	Initial conditions that were due to the previous bad experience with SailPoint IIQ or performing access reviews.
P-PEU	The perception that manager's develop about the ease of use of SailPoint IIQ or the access review component of Sailpoint IIQ.
P-PV	The perception that manager's develop about the value of performing access review on SailPoint IIQ.

Figure 5: Sample of Codes Descriptions

After the processes of coding, searching for themes, reviewing themes, naming, and defining them, the researcher came up with the exhaustive list of themes and sub-themes. Figure 6 reports the themes and sub-themes.

Subject of resistance	Object of Resistance	Initial Conditions	Perception	Resistance Behaviour
Bank Managers	System itself System Significance System Advocates Process	Unclear access Previous experience Lack of top management support User interface Job performance Managers being the wrong audience Lack of consequences Lack of access review training	Perceived wrongdoing Perceived ease of use Perceived consequences Perceived value	Apathy Passive Active

Figure 6: Themes and sub-themes

3.9 Rigour

The aim of an interpretive study is not to test hypotheses; it is to identify, explore, and explain how factors are related and interdependent by looking at how the individuals perceive the world in a social context (Oates, 2006). Therefore, the quality of an interpretive study cannot be judged the same way as that of a quantitative study (Pandey & Patnaik, 2014).

Trustworthiness is the philosophical and methodological assumption that many studies use to assess the quality of the qualitative research results (Anney, 2014). Qualitative studies measure trustworthiness by using a set of criteria (Lincoln & Guba, 1986; Oates, 2006). The criteria as established by Lincoln & Guba (1986) include confirmability, dependability, credibility, and transferability. This study uses the criteria set by Lincoln and Guba (1986) to evaluate the quality of the results.

Confirmability is the degree to which the respondents form the results of an inquiry, and not the researcher's bias, interest, or motivation (Lincoln & Guba, 1985). The study made use of the quotes in the findings evidence to depict that the interpretation came from the participants' responses.

Dependability is demonstrating that the results are consistent and repeatable (Lincoln & Guba, 1985). Repeatability of the work is challenging in qualitative inquiries (Pandey & Patnaik, 2014). To ensure dependability, the study described the analysis process.

Credibility is another criterion for establishing the trustworthiness of the research. Credibility is concerned with the extent to which the research results represent the reality (Pandey & Patnaik, 2014). The researcher is confident that the research results represent reality because the participants' provide evidence that the perceptions presented in the findings represent the reality within the context.

Transferability refers to the extent to which the research results can be transferable to another study or context (Lincoln & Guba, 1986). According to Lincoln & Guba (1986), the thick description is a technique for establishing transferability in qualitative research, when a researcher's description of the phenomenon is thorough, how the study reached its conclusions become visible. The researcher achieved transferability by ensuring that the study provides thick descriptions and providing the description of the research context to ensure that readers can evaluate whether the context they wish

to transfer to is similar or not. Therefore, the researcher is content that the research is transferrable to other contexts.

3.10 Ethical Considerations

This section outlines the ethical considerations for the study, following are the research ethics principles that were applied:

Conflict of interest

The study was conducted for academic purposes only, and there was no financial gain from any supporters. Suppose the case study site requests a presentation of the study results. In that case, the presentation of the results will be without any financial gain, and the presentation will exclude the study participants' identification information.

Permission to conduct study

The business representative(s) at the case study site provided written consent stipulating that the researcher has permission to conduct the study at the site. Moreover, the researcher will follow the conditions stipulated by the case study site representatives in the permissions letter.

Anonymity and confidentiality

The researcher did not share any detail that uniquely identifies the case study site and the study participants in the study. When writing an interview transcript, the researcher substituted any the name of the organisation with 'ABC Bank' for the meaning to remain complete. The researcher will store and will continue to treat all the information obtained during the interviews with anonymity and confidentiality. The researcher stored all the records from the interviews on a password protected device.

Voluntary participation

Participating in the study was voluntary, and the researcher did not offer rewards to the individuals that opted to participate in the study. The researcher informed the individuals that opted to participate in the study that they had an option to withdraw from the study at any given time.

Interview invitations went to the managers that fit the criteria mentioned in the sampling section. The researcher did not pursue managers that displayed a lack of interest to take part in the study or explicitly decline the interview meeting invite.

Disclosure and Informed Consent

The researcher explained the purpose and objectives of the study to the participants beforehand (meeting invite), and at the beginning of the interview. Thereafter, the individuals had to agree to participate in the study by accepting a meeting invite or providing verbal consent. The approach of taking either 'the acceptance of a meeting invites' or 'verbal approval' as consent participate was because signing a consent form became difficult because of COVID-19 rules and regulations. During the time of data collection, the participants were working from home and printing non-work-related documents seemed impractical for them.

Permission to record the interview

Before the interview began, permission to electronically record the interview for transcription and analysis purposes was requested. A disclaimer was made to the participants that sharing of details that uniquely identifies them participating in the study will not happen. The confidential information of the study participants will be kept anonymous.

University of Witwatersrand Ethics process

The ethics process required to be followed by the school of Information Systems ethics committee was followed, and the approval from the committee was gained. The ethics clearance protocol number is CBUSE/1785, The supporting documents are as follows:

- Ethics Clearance Certificate attached in Appendix B
- Consent form attached in Appendix C
- Participation Sheet attached in Appendix D

The permissions letter obtained from the Case Study site was not attached because it was done on ABC Bank's letter head, and it will then compromise the Anonymity and Confidentiality principle if it is attached.

CHAPTER 4: *EMPERICAL FINDINGS: DATA PRESENTATION AND ANALYSIS*

The objective of this chapter is to present the collected data in a logical structured manner. The collected data was presented per concept and provide a discussion of the findings happened per concept.

The section below presents the findings of the study as derived from engagements with study participants through the electronic interviews. A summary of themes and sub-themes that emerged from the study are divided into two sections, generic section, and the main section.

4.1 Contextual Themes

This section of the study summarises the participants' responses to the study's generic questions that sought to understand the participants' understanding of what an access review process is, and what they understand is the use of SailPoint IIQ within ABC Bank. Part of defining the themes and sub-themes, the researcher looked into the collected data and related the findings to the functions of an IGA System under section 1.2 SailPoint IdentityIQ and the access certification/review discussion under section 1.3 Access Certification/Review. The findings are presented in Figure 3.

Access Review Understanding	Use of Sailpoint IIQ
Access Validity	Access Review Access Request Identity Life Cycle Password Management Other

Figure 7: Contextual Themes

4.1.1 Access Review Understanding

The study participants displayed a good understanding of what an access review process is about. The participants provided responses regarding what they believed (mostly based on experience) to be the best description of an access review process.

4.1.1.1 Access Validity

Based on the participants' responses, they believe that an access review is a process that is used to verify and confirm whether user's access is still valid to certain applications, systems, and platforms within the ABC Bank. The quotes from bank managers that demonstrate that SailPoint IIQ is also used for access validity are included below:

> *"It's a recertification to ensure that my staff are still valid to have the access to which they already have." (Middle Manager 2)*
>
> *"Where some of your staff have access to certain platforms within the [ABC Bank] system, and then there's an annual review to see if they are still supposed to have access." (Senior Manager 2)*
>
> *"It's a necessary control to ensure that people who should have access remain to have access and those that should not have access, do not have it. So, this is really a confirmation on a regular basis by managers to ensure that their direct reports have the necessary access that is required." (Executive Manager 2)*

The bank managers understanding of the access review is aligned with what was previously defined by Atyam (2010), and Identity Management Institute (2019). However, Executive Manager 2's understanding is also aligned with the access review importance as highlighted by Zhao and Johnson (2010).

4.1.2 Use of SailPoint IIQ

The study participants displayed to have a good understanding of what SailPoint IIQ is used for within the bank. The participants provided a response of what they believe (mostly based on experience) best describes the uses of SailPoint IIQ at ABC Bank. The participants responses depicted that the participants use or have used SailPoint IIQ for different causes. From the participants' responses, the uses of SailPoint IIQ can be summarised to access review, access request, identity life cycle, password management, and other.

4.1.2.1 Access Review

Based on the participants' responses, some of the participants believe that SailPoint IIQ within ABC Bank is used, amongst other functions, to perform access review, which is what this study is mainly focused on. The quotations from the participants that

described the use of SailPoint IIQ to be performing access reviews as part of their responses to the ‘use’ question include:

“To mitigate the risk of uncertified people” (Middle Manager 4)

“*To certify people's access.” (Senior Manager 1)*

“*It's also used to review access.” (Executive Manager 1)*

SailPoint IIQ fulfils the access review function through its Compliance Manager module.

4.1.2.2 Access Request

According to Gaehtgens et al. (2019), ‘access request’ refers to enabling users to request access through an intuitive user interface. Some of the participants believe that SailPoint IIQ within ABC Bank is used to facilitate the request for access. The quotations from some of the participants that described the use of SailPoint IIQ to be the facilitation of access requests as part of their responses to the ‘use’ question include:

“To simplify the whole access requesting process” (Middle Manager 4)

“It is used for granting the access” (Senior Manager 2)

“To help us provision access” (Executive Manager 3)

SailPoint IIQ fulfils the access request function through its Lifecycle Manager module.

4.1.2.3 Identity Life Cycle

The ‘identity life cycle’ refers to maintaining digital identities from when an identity gets created until it gets archived and deleted (Gaehtgens et al., 2019). The identity life cycle includes but is not limited to the processes of joiners, movers, and leavers (Cameron & Grewe, 2020). Some of the participants believe that SailPoint IIQ within ABC Bank is used to facilitate the identity life cycle. The quotations from the participants that described the use of SailPoint IIQ to be the facilitation of the identity life cycle as part of their responses to the ‘use’ question include.

“The other thing it simplified is for the taking away of the people's access when they leave ABC Bank, and also for giving us a chance as managers to take

away the people's access when they are no longer doing the same job." (Middle Manager 3)

"To grant access to new joiners" (Senior Manager 1)

"To facilitate the joiner, mover, leaver process for access" (Executive Manager 1)

SailPoint IIQ fulfils the identity life cycle request function through its Lifecycle Manager module.

4.1.2.4 Other

There are various other functions that the participants revealed that they believe SailPoint IIQ is used for within ABC Bank. Some of these uses that the participants revealed did not repeat as often throughout the interviews, particularly when participants were asked the 'use' question. Following are some of the quotations of the other uses of SailPoint IIQ that were revealed by the study participants at all management levels, other uses of SailPoint IIQ include:

"It started off as user ID requesting, but it's now unlocking, locking, resetting, passwords, syncing, creating distribution lists, or domain or AD [Active Directory] groups, putting users in AD [Active Directory] groups." (Middle Manager 2)

"There's a reporting component to it as well" (Senior Manager 4)

"It has some components in, like segregation of duties, toxic combinations[3], mandates" (Executive Manager 3)

SailPoint IIQ fulfils these other functions through its Compliance Manager, Lifecycle Manager, and Password Manager modules.

Overall, the responses show understanding of the system's functionalities as outlined in section 1.2 SailPoint IdentityIQ.

[3] Toxic Combination refers to an automated way to prevent and remove access that when given together present a high risk to ABC Bank

4.2 Main Analysis

This section of the study analyses the participants' responses to the study's main questions that were derived from the conceptual framework and the influential literature. In the interview protocol, the objective of the main questions was to understand and explain why bank managers resist the access review component of SailPoint IIQ within ABC Bank. The findings are presented in Figure 6: Themes and sub-themes.

4.2.1 Subject of Resistance

According to Lapointe and Rivard (2005), this is individuals, groups, or organisations that adopts the resistance behaviour. The study identified the subject of resistance as the managers of all the levels from middle management, senior management, to executive management. Within ABC Bank, middle managers, senior managers, and executive managers are the individuals that are required to perform access reviews for their subordinates. Participants' responses that show that all levels of management are subjects of resistance include:

> *"I resist the fact that I think a number of items are being done, when there is no good reason to do it." (Middle Manager 2)*
>
> *"I just cannot make sense of the access that my staff have, simply because the access displayed in the recertification screens does not make any business sense … I mean when you have this weird thing and a decision is expected from me in a specific time to approve or revoke their accesses, it is just unreasonable." (Senior Manager 2)*
>
> *"If I have to prioritize this, I do not see what the value of this is and I have got other more important things" (Executive Manager 3)*

Rivard and Lapointe (2012) posit that resistance to information systems can be in different levels of management, for example, business managers, divisional managers, operations head, supervisors, senior managers, and top management. The results of this study agrees with the findings by Rivard and Lapointe (2012).

4.2.2 Object of Resistance

According to Lapointe and Rivard (2005) the objects that individuals, groups, and organisations can resist are: a system itself, system advocates, system significance.

’Process’ as an object of resistance was inductively added based on the participants’ responses.

4.2.2.1 System Itself

The system itself represents the specific features within the system, and the users tend to resist the features that do not meet their expectations (Selander & Henfridsson, 2012). This object of resistance was noted by participants from all levels of management, the responses that the participants’ provided that relate to the ‘System itself’ when they were asked what they believe managers are resisting mainly related to ease of use.

> *“The ease of use, I should be able to log in, understand what’s being asked of me and perform the task easily and efficiently” (Middle Manager 1)*
>
> “*Bank managers are resisting the system due to it not being user friendly” (Senior Manager 2)*
>
> *“I would say that most managers are resisting the System and its functionalities. If I can add to that, some are resisting the system configurations that are not working, which makes them not to use the system for access requests and approvals or perform recertifications” (Executive Manager 1)*

In the above quotations, the middle manager stated that system is not easy to use. From a senior management perspective, some of the senior managers also believe that the SailPoint IIQ is not user friendly, hence the resistance. Some of the managers, as per an executive participant, are resisting SailPoint IIQ because they believe there are configuration issues in the system itself. This supports Selander and Henfridsson (2012) results whereby users of the system were resisting a system because of configuration problems and usability of the system and functionalities.

4.2.2.2 System Significance

System significance represents that individuals resist a system because of the meaning they ascribe to adopting the system (Selander & Henfridsson, 2012). This object of resistance was noticed by participants from all management levels. The responses that some participants provided during the interviews regarding system significance include:

"*I resist the fact that I think a number of items are being done, when there is no good reason to do it" (Middle Manager 2)*

"S*o often it is somebody coming around with a big stick to say, you need to use this tool" (Senior Manager 3)*

"Why do I need to do this?" (Executive Manager 3)

From the above, a middle manager revealed that some of the managers do not perform access reviews on SailPoint IIQ because they do not see the importance or reasons behind it. One of the senior management participants believe that the importance of using SailPoint IIQ to perform access reviews is not known by managers because 'top management' just brought the tool to the managers and said they must use it without imparting the knowledge regarding the 'why'. This supports the existing literature by Selander and Henfridsson (2012), the mangers resistant because they do not see the necessity, importance, or rationale for performing access reviews on SailPoint IIQ, the meaning that they have put t it is that it is not a useful tool.

4.2.2.3 System Advocates

System advocates posit that individuals resist the entire system's implementation process based on who is at the forefront of the system implementation (Selander & Henfridsson, 2012). This object of resistance was noted by one of the senior managers, the participant stated,

"I don't want to say some people in the CIB [Corporate Investment Banking] space resist the [Technology space[4]] per se because this is not the first time they bring in a platform without involving us and some platforms just do not work well with our platforms" (Senior Manager 1)

This statement highlights that the senior manager believe that some of the managers within the CIB space resist performing access reviews on SailPoint IIQ because they have been getting platforms or Systems from the Technology space of ABC Bank without their involvement or knowledge. This is in support of the literature by Selander and Henfridsson (2012), however, this theme came through less strongly than the others themes.

[4] 'Technology Space' refers to the IT Division/Business Unit within ABC Bank.

4.2.2.4 Process

Additionally, some of the participants highlighted that the some of the managers do not necessarily resist the system itself, system significance, and/or system advocates. The participants believe that they resist the process in its entirety. The process has been defined in this study as the implicit activities involved in performing an access review, these are the steps that some managers believe are the 'best' for performing an access review correctly. Participants of different levels of management noted this as an object of resistance, their responses include:

> *"There was no easy way for him [Participant's Manager] to go through the process" (Middle Manager 1)*
>
> "*They resist the process in its entirety, what do I mean by that? They resist having to spend a lot of time finding out what they are certifying, which is a very daunting process" (Senior Manager 2)*
>
> *"[It] definitely is a cumbersome process." (Executive Manager 2)*

From the above, a middle manager participant revealed that there was a time where his manager was upset with performing his access review because there was no easy way for him to perform the access review. The participant's manager had to go through an experience of sitting with him trying to understand the access that he had in various systems, and it was not a good experience for the manager, as a result the participant believes that some managers can resist the process that they must go through during an access review. A senior manager participant also believe that some managers resist the process of trying to find out what access their subordinates have to various systems. Some participants postulate 'technical access names'[5] and 'lack of (descriptive) descriptions'[6] is the reason why managers must find out what the access their subordinates have. An executive participant highlighted that the access review process itself is a cumbersome process, hence this participant believes that managers can resist the process itself as a result.

[5] 'Technical access names' refers to the access that is granted in the System's back end. For Example, a technical access name for 'Analyst Access' to a trading system can be '\\A-OCR-@#QQD', which is does not explicitly say 'Analyst Access' to a trading system.

[6] SailPoint IIQ has a functionality where administrators can describe access and what it does so that when Access Reviewers (Managers) are reviewing their subordinates' access, they can know what they are reviewing. Additionally, description of access also aids the employees when they request for access, they can know what they are requesting access to.

4.2.3 Initial Conditions

The study defines initial conditions as the subjectivities that managers possess at an individual level. It includes the already existing inputs and outputs, the established power and political structures, work routines, organisational structures, and individuals already existing perceptions and views about SailPoint IIQ and access reviews. Unclear access, previous experience, lack of top management support, user interface, job performance, managers being the wrong audience, lack of consequences, lack of and access review training are the initial conditions that were categorised based on the participants' responses.

4.2.3.1 Unclear Access

Some of the participants highlighted that one of the things that already exist in the system and has a potential to lead bank managers to not perform access reviews on SailPoint IIQ is that the system consists of unclear access. According to participants, access becomes unclear because of 1) technical access names that are not business friendly for managers and 2) lack of descriptive access descriptions. This was noted by managers at all levels, quotations from the interviews include:

"It takes time to find out what those technical names mean, and not everyone is willing to make that time" (Middle Manager 4)

"When doing recertification, it's like we are recertifying some back-end code that I think some developer has written, that is not business-friendly at all, as managers we want simple things, I understand the lack of descriptions, but you can at least give me a descriptive name of the access." (Senior Manager 2)

"*Lack of access descriptions … makes managers to not perform recertifications on SailPoint IIQ." (Executive Manager 1)*

According to Friedman (2018), when access is not clear for managers, it often leads to confusion during access certifications and some managers can behave passively.

'Unclear access' has a relationship with 'Process' because part of the process that managers typically take if there is unclear access that the manager is reviewing is to sit down with the subordinates and ask them if they need the access, the other process

include managers asking around what the access does. ‘Process’ and ‘Unclear access’ would typically interplay for the manager to develop a perception.

4.2.3.2 Previous Experience

Previous or prior experiences has been studied to be a cause of resistance (Ali et al., 2016; Del Val & Fuentes, 2003; Ford & Ford, 2009). Some participants highlighted that some previous experiences that managers had with the system itself can lead managers to resisting the access review component of SailPoint IIQ. Some also highlighted that some previous negative experience that some managers have encountered when performing access reviews on SailPoint IIQ can also lead managers to not performing access reviews on SailPoint IIQ. This has been noted by managers at middle and executive levels: Quotations from the interviews include:

> *“When I think of [SailPoint IIQ], the first thing I think about is those technical difficult names that I have to interpret. So, it makes me already have this attitude… So, you tend to automatically have this negative vibe towards [SailPoint IIQ]” (Middle Manager 4)*

> *“Configuration errors or feeds issues are leading people to not doing recertifications because you know, people don't want to use a solution that does not work for them” (Executive Manager 1)*

Ali et. al (2016), and Del Val and Fuentes (2003), refer to previous or prior experiences as ‘Past failures’. This study supports the existing literature regarding this initial condition. ‘Previous experience’ has a relationship with the ‘System itself’ because, based on the responses, the experiences and failures that managers have encountered with SailPoint IIQ or the access review functionality itself can be attributed to the system itself by managers. Therefore, ‘Previous experience’ and ‘System itself’ would interplay for managers to develop a perception.

4.2.3.3 Lack of Top Management Support

Lack of top management support has been studied to be amongst some of the causes of user resistance (Ali et al., 2016; Del Val & Fuentes, 2003; Kim & Kankanhalli, 2009; Landaeta et al., 2008). Some participants highlighted that there is a lack of top management support that they have noticed within their departments and divisions. Some of the participants’ highlighted that within their departments and divisions, top

management stress the importance of performing access reviews. The quotations from participants of middle and senior management include the following:

> *"I've seen senior managers go, I'm not using that crap just to recertify the people. Okay? and that is a message that comes down to me as a first, line manager, you know, if a CIO in the bank won't use it, why should I use it?" (Middle Manager 2)*

> *"Sometimes if there is not a top-down support for these reviews… we as subordinates will not go and perform the process either" (Senior Manager 4)*

In the initial conditions highlighted in the causes of resistance section, Rumelt (1995) highlighted this initial condition as 'Leadership inaction' and 'Inadequate strategic vision' because senior and executive managers do not seem to be showing commitment and promoting SailPoint IIQ as a tool to perform access review from a strategic point of view. Instead, some top managers, explicitly express their how they do not support the performing access reviews on SailPoint IIQ, which ultimately leads to lower-level managers not performing access reviews because they are following their leader.

'Lack of top management support' has a relationship with 'System significance' and 'System advocates'. Regarding 'System significance', lower-level managers can view a superior (Senior or Executive manager) expressing how they do not perform access reviews on SailPoint IIQ and develop a perception of 'value', basically, whether the system adds value to them or the organisation. Regarding 'System advocates', lower-level managers (with the CIB space for Example) can view a superior (Senior or Executive manager) not using SailPoint IIQ or performing access reviews on it and develop a perception that there are no consequences to not using SailPoint IIQ because it is from the Technology division of ABC Bank.

4.2.3.4 User Interface

User friendliness or perceived ease of use has been studied to be one of the contributors to user resistance (Davis, 1989). Participants in the study highlighted that SailPoint IIQ user interface is not user friendly for most of the managers. Moreover, they also believe that bank managers believe that the interface of the Access Review component of SailPoint IIQ is not user friendly. The user friendliness has been noted

by participants at all levels of management. The participants' responses regarding user friendliness include:

> *"The interface is extremely un-user friendly to be able to do recertifications" (Middle Manager 2)*
>
> *"I think it's not user friendly in how we're using the codes to represent the access people have" (Senior Manager 2)*
>
> *"The recertification component of the system is not very intuitive or user friendly" (Executive Manager 1)*

The 'User interface' has a relationship with the 'System itself' because when managers interact with the screens or user interface of SailPoint IIQ or the access review component of it, the perceptions that they develop about what they see are attributed the user interface. 'User interface' and 'System itself' would interplay for a manager to develop a perception.

4.2.3.5 Job Performance

Some participants believe that managers do not perform access reviews because it is not a task that they get rated against during their job performance reviews. They also believe that access reviews are a time-consuming task and if they are to prioritise it against other tasks that they get rated on, they will prioritise other tasks. This relates to initial conditions because managers' job scorecards/performance matrices already exist but without a performance indicator that measures at performing access reviews on SailPoint IIQ. This was noted by participants at all management levels, the quotations from some of the participants include:

> *"Most guys that I've seen, and this includes myself, when I don't do it is, it doesn't form or it doesn't feel like it forms part of my normal day to day, and it's just a cumbersome thing that gets in the way of actually doing things where you feel the things that require your attention more" (Middle Manager 1)*
>
> *"People are sometimes swamped, and you know, where does this lie in their priority of things to do?" (Senior Manager 3)*
>
> "O*ther people might just feel like it takes a lot of effort for them to do recertification for their people which is basically what they are not hired to do,*

which in essence will not necessarily make them better off during their performance reviews" (Executive Manager 1)

'Job performance' and 'Process' have a relationship because, based on the responses, when some managers view the performing access reviews, they think of how time consuming and cumbersome the exercise is. 'Job Performance' and 'Process' would interplay for a manager to develop a perception.

4.2.3.6 Managers Being the Wrong Audience

Some of the participants pointed out that managers are not always the correct audience for performing access reviews. This was noted by participants at middle and senior management levels, some quotations about managers not always being the correct audience include:

"I own some AD [Active Directory] groups, and I can certify who is within those groups, and as the owner of that group, I should know what that group does, and I should know who's in it, and who should be in it, and I'm comfortable with that recertification. I'm not comfortable, where I am not the owner, but I also have to perform a recertification" (Middle Manager 2)

"There is a part of me that wonders why these recertifications must always be on a line manager basis. But I actually know my process better so why can I not grant access to people that I know should be having access to my system, so the model is very narrow, narrow in a way that it's always a line manager process, and I think that's a huge shortcoming. That is why on my system, recertifications will be done by team administrators, cost centre owners, and financial managers" (Senior Manager 2)

'Manager being the wrong audience' and 'Process' have a relationship because, based on the responses, some managers view the process of performing access reviews to be incorrect because ABC Bank makes the primary access reviewer to be the immediate line-manager. 'Manager being the wrong audience' and 'Process' would interplay for a manager to develop a perception.

4.2.3.7 Lack of Consequences

The participants of different management levels believe that the current lack of consequences contribute to the managers resistance of the access review component

of SailPoint IIQ. This was noted by participants at all levels of management, some quotations from the participants' responses include:

> "*Irrespective of whether I actually approve it or not, it doesn't make any difference, because there's no consequences and nothing happens anyway." (Middle Manager 2)*
>
> "*If I skip a recertification? What would the consequences be like? …your access will be lost right? We know that doesn't happen, there is no consequences if you don't do it" (Senior Manager 2)*
>
> *"Some managers know that there are not consequences for not doing recertification for their staff." (Executive Manager 1)*

'Lack of consequences' has a relationship with 'System significance' because, based on the responses, some managers view the performing access reviews on SailPoint IIQ to be less important than other tasks that have consequences if they do not perform them. 'Lack of consequences' and 'System significance' would interplay for a manager to develop a perception.

4.2.3.8 Lack of Access Review Training

Participants of different management levels believe that the lack of training that is specific to access reviews might contribute to the managers resistance of the access review component of SailPoint IIQ. This was noted by participants at all levels of management, some quotations from participants' responses include:

> *"I think there's a training component that I think that is missing with the tool…" (Senior Manager 4)*
>
> *"I think I have not seen any training specifically for recertification" (Executive Manager 1)*

The participants of senior and executive management levels believe that there is a training component that is missing, which potentially could lead to resistance because people might not have the knowledge on how to perform access reviews. However, a middle manager participant highlighted that there is some level of training for SailPoint IIQ, however, the training is not specific to performing access reviews but mostly on requesting for access. Following is the middle manager's quotation:

"I have done a lot of trainings for different systems… So, nearly all of those trainings, there is a part where they present how you go about requesting for access to the platforms we are being trained on, those parts have screens of [SailPoint IIQ], the first part of those things is about how to get into [SailPoint IIQ] to request for this or do that, I can't think of one training that I attended recently which does not have a [SailPoint IIQ] section in it. Now I know most of the [SailPoint IIQ] stuff by heart because of the trainings I attended" (Middle Manager 4)

The above suggests that the senior and executive management participants were talking about the lack of training that has been tailored specifically for access reviews.

4.2.4 Perception

When an object of resistance and initial conditions coincide, managers develop a perception that can ultimately lead them to behaving in a resistant manner.

4.2.4.1 Fear of Error

Some participants highlighted that some of the managers do not complete the access reviews on SailPoint IIQ because the access that they are reviewing does not have business friendly names or descriptions that tells them what the access does. Some participants believe that if they complete an access review on access that is not clear they might end up approving or revoking the access they were not supposed to approve or revoke, which might open the bank to more risk. A middle manager participant said,

"The motivating issue could be running away from risk, like from my point of view, I would rather not recertify someone if I do not understand what I am recertifying than to certify them and realise I did something wrong" (Middle Manager 4)

The individuals' inherent values do not allow them to perform access reviews for the sake of performing access reviews without knowing what it is that they are certifying.

4.2.4.2 Lack of Perceived Ease of Use

According to other participants' responses, the perceived ease of use of the System itself or the access review component can lead managers to behaving in a resistant

manner, some participants highlighted that the unclear access is the factor that leads to the un-user friendliness of the system. A middle manager participant said,

> *"I don't want to say the system is not friendly or it is hard to use, but the descriptions of access can make it difficult" (Middle Manager 3)*

Based on the middle manager comment, lack of the descriptions makes the access review component difficult to use. However, an executive manager participant stated that even SailPoint IIQ itself is not user friendly.

> *"I personally think that the System itself and the recertification component of the system is not very intuitive or user friendly. But I use it because for me it is literally part of my job" (Executive Manager 1)*

Based on the executive manager's comment, if performing access reviews was not part of their jobs, they likely would not perform the access reviews. Therefore, for people that perceive SailPoint IIQ or the access review component as un-user friendly, and access reviews are not part of their jobs, they are likely to behave in a resistant manner.

The individuals develop a perception about access reviews based on the system inherent factors which in this case is the user interface. 'Perceived ease of use' concept was also studied by Davis (1989) and postulates that how users perceive the system to be easy to use can influence how they perceive the system to be useful, and ultimately influence their intention to use a system.

4.2.4.3 Lack of Perceived Consequences

Some managers resist performing an access review on SailPoint IIQ because they believe that the functionality for taking access away does not function properly, so these managers believe that whether they complete an access review on SailPoint IIQ will not make any difference. A senior manager participant said,

> *"If I skip a recertification? What would the consequences be like? …your access will be lost right? We know that doesn't happen, there is no consequences if you don't do it" (Senior Manager 2)*

Based on the above, previous experience with SailPoint IIQ and performing access reviews on SailPoint IIQ affirmed to the managers that the promise to take away the access on non-performance of the access review does get fulfilled by SailPoint IIQ.

Additionally, some participants believe that some managers do not perform access reviews because they believe that SailPoint IIQ itself is not a reliable system as some of the functionalities or configurations do not properly function. An Executive manager participant said,

> *"I would say that most managers are resisting the System and its functionalities. If I can add to that, some are resisting the system configurations that are not working, which makes them not to use the system for access requests and approvals or perform recertifications" (Executive Manager 1)*

Therefore, participants believe that some managers do not perform access reviews mainly because they perceive that there are no consequences if they do not perform access reviews for their subordinates.

The individuals develop a perception about access reviews because their people characteristics and system characteristics conflict. Their people characteristics can be seen as the experience they have with SailPoint IIQ and/or its access review component. The System characteristics can be seen as how they perceive the reliability and user interface of SailPoint IIQ and/or its access review component. When the two characteristics (System and people) conflict in the managers' mind, they will perceive it as unfavourable. For example, their experience is already negative about SailPoint IIQ, when they notice that the system configurations do not work properly, they end up with a perception that, even if they do not perform an access review on SailPoint IIQ, nothing tangible will happen because there are configuration issues.

4.2.4.4 Lack of Perceived Value

Some participants believe that some managers do not perform access reviews on SailPoint IIQ because they believe that it is a cumbersome and tedious exercise that is time-consuming, and they do not see the value it adds to their jobs or the organisation. Some do not perform the access reviews because they believe that it does not add value to their jobs and as a result, they put less priority on performing access reviews. Some participants think that some managers just believe that they were not hired to perform access reviews due to the effort that it requires, and they would rather prioritise their primary job responsibilities than prioritising performing access reviews. An executive manager participant said,

“I think there is just also a component of managers not doing it because they don't see the value of it. They do not really understand why this is important and in the amount of things they have to do they prioritize are looking at, I mean, I'm sure your stuff that comes on to your queue, you have to constantly prioritize because there is always more to do than what there is time” (Executive Manager 3)

The individuals’ inherent values do not allow them to perform access reviews for the sake of performing access reviews because it takes away from the time that the managers believe they can be doing work that contributes to their job performance. For example, if managers values getting a good performance rating, and they perceive performing access reviews as a cumbersome and time-consuming task that is not functional, they will not perform an access review, they would rather do more of their work.

4.2.5 Resistance Behaviour

The resistance behaviours that the have been noticed by the participants of all levels include apathy, passive, and active resistance behaviours.

4.2.5.1 Apathy

Some participants believe that the resistance behaviour that is exerted towards the access review component of SailPoint IIQ is apathy. They believe that some managers are still indifferent about performing access reviews on SailPoint IIQ. Quotations from participants relating to the apathy behaviour include:

“I've been asked to certify… I got to a point where I was a bit indifferent about the system itself… when they send the information, they give you technical information” (Middle Manager 4)

The middle manager was indifferent about the system itself because what was being asked of the participant was to perform an access review on an unclear access. The participant believed that some managers could behave in an apathetic way towards the access review component of SailPoint IIQ because of that. Moreover, an executive manager participant said,

“They're indifferent about doing these reviews when it is needed because it is just one of those things, it's not anyone's daily job” (Executive Manager 2)

The executive manager believe that some managers are just indifferent about performing access reviews on SailPoint IIQ because it is not part of their daily job. Additionally, other participants also mentioned that performing access reviews is a cumbersome and time-consuming task, which also adds to the managers behaving in an apathetic way.

4.2.5.2 Passive Resistance

Some of the participants believe that a passive resistance behaviour is exerted by some of the managers, which means that they believe that some managers do not perform access reviews on SailPoint IIQ because they always have an excuse for not completing access reviews on SailPoint IIQ. One of the executive managers said,

> *"There is just also a component of managers not doing it because they don't see the value of it… if I have to prioritize this, I do not see what the value of this is and I have got other more important things in their mind to do" (Executive Manager 3)*

The executive manager believes that some of the managers will put less priority on performing access reviews mainly because they do not see the value it adds either towards the organisation or to their job performance.

4.2.5.3 Active Resistance

Some participants believe that some managers actively resist completing access reviews on SailPoint IIQ, let alone using the system itself. One of the middle managers stated that,

> *"I say they are resisting the system is because one can request for access… and the responsible approvers would sit with the item to approve for so long, when you follow up with them, they ask you, why did you log the request via [SailPoint IIQ]? What happened to filling up forms? this system does not work, you must fill up the form and send it to me, I will sign and you will get the access" (Middle Manager 3)*

Based on the above, the responsible approvers are actively on a mission of not making SailPoint IIQ be used by other people, which is a definition of active resistance. An executive manager also said,

> *“There's a lot of us managers that talk to each other about this system… so managers convince each other… that this thing is broken, is not working, and therefore they're not gonna do it.” (Executive Manager 1)*

This executive manager believed that some managers are even going to an extent of convincing each other to not perform access reviews on SailPoint IIQ because they have had some challenges with the system, and they believe that it does not work or function properly.

4.3 Conclusion

Overall, it was highlighted that the reason why the bank managers resist the use of the access certification component of SailPoint IIQ lies in the interplay between the initial conditions and the object of resistance. The reason can be classified as the perception that is developed after interaction between initial conditions and the object of resistance.

The initial conditions that were identified during the data analysis are unclear access, previous experience, lack of top management support, user-friendliness, job performance, managers being the wrong audience, lack of consequences, and lack of access review training.

The objects of resistance that were identified during the analysis of data are the system itself, system significance, system advocates, and the access review process.

The perceptions that typically develop and ultimately lead to the resistance behaviours by managers were identified to be fear of error, lack of perceived ease of use, lack of perceived consequences, and lack of perceived value. These perceptions typically lead bank managers to behave in either of the resistance behaviours namely apathy, passive resistance, or active resistance.

CHAPTER 5: *DISCUSSION*

The aim of the study was to understand why some bank managers resist or do not use the access review component of SailPoint IIQ within the context of a South African Bank. The findings discussed in the previous chapter helped in the understanding of the subject and its relationship to literature.

5.1 Interpretation

The findings of this study uncover some concepts that can be considered when studying user resistance related to an IGA solution. The study uncovered the findings by applying an amended version of the framework by Lapointe and Rivard (2005). By applying this framework, the researcher uncovered various initial conditions, objects of resistance, perceptions, and resistance behaviours that relate to an IGA solution.

5.1.1 Subject of Resistance

The findings identified subjects of resistance to be middle managers, senior managers, and executive managers, as these are the individuals that are required to perform access reviews on SailPoint IIQ at ABC Bank.

5.1.2 Initial Conditions

The findings depict that there are several factors that play a part in how bank managers view the access review component of SailPoint IIQ. The examples of these factors include 1) the lack of top management support in some departments within the ABC Bank which affects how subordinate managers perceive the importance of performing access reviews, and 2) the existence of unclear access within SailPoint IIQ which affect how managers perceive the complexity of performing access reviews.

The study reveals that in as much as there are various factors that exist and are not understood, resistance behaviours from some managers are likely to noticed. However, the researcher also uncovered that ‘use’ does not necessarily equate to ‘acceptance’ of the current situation, which might ultimately lead to more resistance in the future. Some participants stated that they perform access reviews, but they are not happy with how it is currently. When organisations respond to resistance, initial conditions can be altered (Rivard & Lapointe, 2012), therefore managers might then accept the solution. For example, if ABC Bank make the access clearer in SailPoint

IIQ, some managers may no-longer be frustrated by the unclear access and will know exactly the access that they are reviewing.

Some of the initial conditions that have been identified empirically are very specific to the resistance that is exhibited by managers towards an IGA solution or an access review component of an IGA solution. The study identified 'initial conditions' that can be considered for research on resistance or adoption of access review component of an IGA solution, the specific 'initial conditions' that have been identified are:

- Unclear access
- Managers being the wrong audience
- Lack of consequences
- Lack of access review training

The above was discussed in detail in the findings. The other initial conditions have been studied in previous resistance literature as contributing to the causes of resistance.

5.1.3 Object of Resistance

The findings depict that there are four objects that interplay with bank managers' initial conditions and affect how they perceive an access review component of SailPoint IIQ. The objects that have been observed by the study are the system itself, system significance, system advocates, and process. 'Process' has been identified empirically, and was not explained by Rivard & Lapointe (2012). With Process for example, a middle manager participant stated that during one of the access reviews, his manager was not pleased by the 'process' of having to set up one-on-one meetings with his subordinates to perform access reviews effectively. In this case, the 'process' object of resistance interplays with an initial condition of 'unclear access', and if this initial condition does get altered as Rivard and Lapointe (2012) suggest, the following time the manager performs an access review, there will also be a 'previous experience' initial condition that comes into play on how the manager perceives the access review component of SailPoint IIQ.

5.1.4 Perception

'Perception' is a new concept for this study, the original model by Lapointe and Rivard (2005) studied 'perceived threat' which are negative consequences that the users

perceive. Studying ‘perception’ instead of ‘perceived threat’ allowed the study to reveal perceptions beyond those that are viewed by managers as a threat. For example, fear of error, is perceived as a threat, however, lack of perceived ease of use, lack of perceived consequences, and lack of perceived value are perceptions that are not viewed as threats by managers, but they can influence managers to behave in a resistant manner.

The findings on this study revealed that managers perceptions about an object of resistance also depend on the interplay between an ‘object of resistance’ and ‘initial conditions’ that exist. Empirically, the study identified four main perceptions that play an influential role on how the managers behave or the severity of the resistance behaviour. The identified perceptions include fear of error, lack of perceived ease of use, lack of perceived consequences, and lack of perceived value. Previous literature studied perceived ease of use, and perceived value/usefulness. The fear if error and lack of perceived consequences are some of the perceptions that the study have identified to be related to performing access reviews on an IGA solution.

To further the above example, when there is an interplay between ‘initial condition’ of ‘unclear access’ and the ‘object of resistance’ of ‘system itself’ (in this case an access review component), a manager from an ‘Accounts Payables Department’ might perceive that if they just approve the access that a user has, a user might commit some fraudulent transaction by having more access than they need, and if they revoke the access, the user might not be able to work the following day, so, in this case, the manager might be somewhat indifferent of what to do, and in the same time they might they are fearful of doing something wrong (**fear of error**). Therefore, based on the perception they developed as a result; it will determine how they behave.

5.1.5 Resistance Behaviour

The findings depict that there are three noticeable resistance behaviours that can be observed from bank managers with regards to how they behave towards the access review component of SailPoint IIQ. The behaviours are apathy, passive resistance, and active resistance; these are three of four behaviours that were studied by Coetsee (1993). The fourth behaviour from Coetsee (1993) taxonomy is aggressive behaviour, this behaviour has not been observed within ABC Bank by any of the study participants. The severity of the resistance behaviour is influenced by the ‘perceived threat’ and it

is often realised in cases whereby the 'perceived threat' is the distribution of power within an organisation (Lapointe & Rivard, 2005). In the context of this study, performing access reviews on SailPoint IIQ does not seem to distribute any powers within the ABC Bank, and the findings support that.

5.2 Updated Conceptual Framework

The findings of this study resulted in the necessity to further develop on the conceptual framework. The text that has been highlighted in blue in Figure 7 show additions to the conceptual framework.

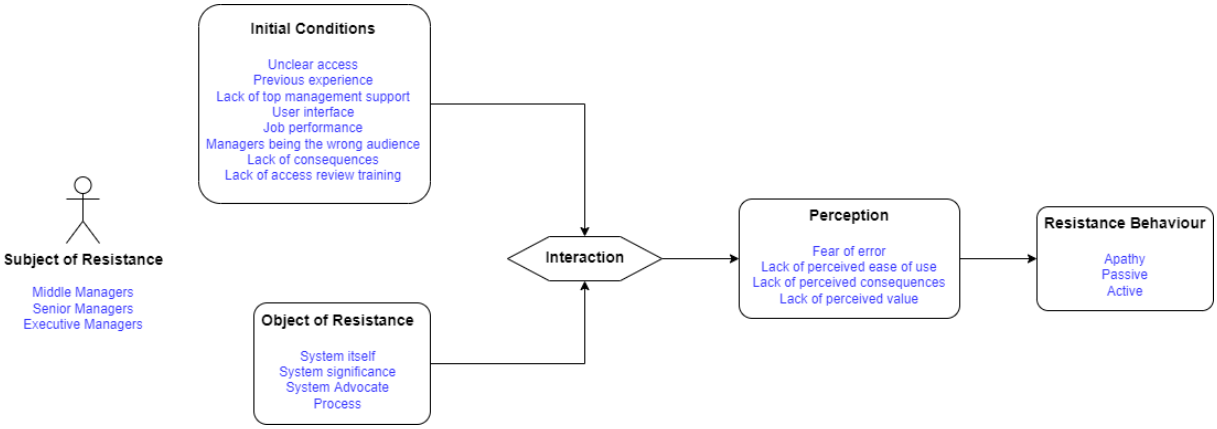


Figure 8: Updated Conceptual Framework

The updated framework is still aligned with the with the conceptual framework that was adopted from Lapointe and Rivard (2005) and used as a theoretical lens for the study. According to the updated conceptual framework, it can be noticed that whenever there is an interplay between initial conditions and the object of resistance, a manager (Subject of resistance) develops a perception that influences how s/he behaves.

The following section reflects on the use of the framework by Lapointe and Rivard (2005) as a theoretical lens and how the framework's concepts were useful in answering the research questions.

Subject of Resistance – This concept allowed the researcher to identify the exact management levels that exhibit the resistance behaviour towards an access review component of SailPoint IIQ.

Object of Resistance – This concept enabled the researcher to identify what the managers are resisting, while answering the research question “What do bank managers resist?”

Initial conditions – This concept of the framework allowed the researcher to identify the existing things that can influence managers to not perform access reviews on SailPoint IIQ, it also enabled the researcher to answer the research question, “What influences bank managers not to perform access reviews?”

Perception – Lapointe and Rivard (2005) studied ‘perceived threat’ which is limited to the negative consequences that the users can perceive after the interplay between an ‘initial condition’ and an ‘object of resistance’. The only ‘perceived threat’ that the study observed was ‘fear of error’, but there are other perceptions that can lead managers to behave in a resistant manner that were revealed by studying the concept of ‘perception’ instead of ‘perceived threat’. This concept allowed the researcher to answer the primary research question, “Why do bank managers resist the use of the access certification component of SailPoint IIQ?”

Resistance behaviour – This concept allowed the researcher to identify how the managers behave towards an access review component of SailPoint IIQ. Moreover, it enabled the researcher to answer the research question, “How do bank managers behave towards the access review component of SailPoint IIQ?”

Overall, the framework by Lapointe and Rivard (2005) was useful in answering the primary and secondary research questions of this study. Moreover, while ‘perceived threat’ is an important concept of the model, it is also essential to note that resistance behaviour is not solely influenced by ‘perceived threats’ only, ‘perceptions’ too can influence resistance behaviour.

CHAPTER 6: *CONCLUSION AND RECOMMENDATION*

The objective of this chapter is to highlight the main purpose of the study and how the study achieved this purpose, and thereafter provide some recommendations. The chapter will do so by outlining the purpose of the study, outlining which research questions were addressed by the study, and what the findings are on the research questions. After that, the chapter will then provide recommendations.

6.1 Summary to research questions answers

The purpose of this study was to examine and explain why some bank managers do not complete access reviews for their subordinates using the access review component of SailPoint IIQ. The following research questions had to be answered to gain an understanding on why bank managers resist using the access review component of SailPoint IIQ.

The primary research question for the study was:

> *Why do bank managers resist the use of the access certification component of SailPoint IIQ?* ***[Perception]***

The secondary research questions were:

- *What influences bank managers not to perform access reviews?* ***[Initial Conditions]***
- *What do bank managers resist?* ***[Object of Resistance]***
- *How do bank managers behave towards the access review component of SailPoint IIQ?* ***[Resistance Behaviour]***

6.2 What do bank managers resist?

The study outlined that the managers resist:

- The system itself (SailPoint IIQ and the Access Review Component)
- The system significance
- The system advocates and,
- The access review process

6.3 What influences bank managers not to perform access reviews?

The empirical data analysis made it evident that there are several existing things that influence managers to not perform access reviews on SailPoint IIQ. Following is a summary of existing things that influence managers to not perform access reviews on SailPoint IIQ:

- The existence of unclear access in SailPoint IIQ.
- The managers' previous negative experience with SailPoint IIQ itself and/or the access review component of SailPoint IIQ.
- The lack of top management support in other divisions.
- User-friendliness
- Managers not getting measured against performing access reviews during the job performance reviews.
- Managers being the wrong audience of some access reviews.
- The inexistence of a consequence system, for example, managers getting a lower performance rating for not performing access reviews.
- The inexistence of the access review training specifically for managers.

6.4 How do bank managers behave towards the access review component of SailPoint IIQ?

The empirical data analysis also made it evident regarding how managers resist the access review component of SailPoint IIQ. The analysis indicated that bank managers exert three resistance behaviours toward the access review component of IIQ, the behaviours are apathy, passive resistance, and active resistance.

6.5 Why do bank managers resist the use of the access certification component of SailPoint IIQ?

Based on the findings, some of the ABC bank managers do not perform access on SailPoint IIQ because of perceptions formed due to the interaction between object of resistance and initial conditions. The empirical data analysis revealed that bank managers can form the following perceptions:

- They perceive that performing access review without the knowledge or clear picture of the access they are reviewing could lead them to doing something wrong **(Theme: Fear of error)**.
- They perceive SailPoint IIQ and its access review component to be difficult to use **(Theme: Lack of perceived ease of use).**
- They perceive that there are no consequences for not performing access reviews **(Theme: Lack of perceived consequences).**
- They perceive that access reviews do not add any value to themselves **(Theme: Lack of perceived value).**

This study focused on the factors that are influencing managers not to perform access reviews on SailPoint IIQ. The case study drew these factors from the various bank managers because managers are the ones that generally perform access reviews for their immediate subordinates within ABC Bank.

As discussed in the previous chapters of this study, it is evident that the primary research question has been answered through by exploring and explaining what the managers' perceptions are after the interplay between initial conditions and object of resistance.

6.6 Theoretical and Practical Contribution

The study revealed that the literature in existence is not enough to explain the user resistance exerted towards a specific component of the system, specifically the access review component of an IGA system. Chapter four provides details of the findings and analysis. Thus, the analysis of this study adds to the existing literature by identifying the factors that influence user resistance to an access review component of an IGA system, and more specifically in the banking sector. Therefore, the contribution of this study is divisible in two: practical recommendation and future research.

6.6.1 Practical recommendation

Practically, this study provides several factors influencing user resistance to the access review component of an IGA System. The study also presents an opportunity for organisations implementing or considering implementing an IGA solution that has an access review component to develop strategies that might mitigate the risk of user

resistance towards an access review component from manifesting. It is therefore recommended that efforts must be focused on:

- **The existence of unclear access in SailPoint IIQ.**

The efforts of making sure that the access that reside on SailPoint IIQ is clear enough for managers. Based on the participants' responses, this can be achieved by ensuring that access contains business friendly names and also a business friendly descriptive descriptions that outlines the permission or privileges that the access grants to specific systems. Friedman (2018) stated that it is important to describe access in a business-friendly manner.

- **The managers' previous negative experience with SailPoint IIQ itself and/or the access review component of SailPoint IIQ.**

The efforts of sitting down with some managers to focus on the opportunities of improvement to address the negative experiences that the managers previously had. Friedman (2018) outlined that it is important for organisations to solicit feedback regarding the delivered projects, and the feedback can be used to improve the solution.

- **The lack of top management support in other divisions.**

Kim and Kankanhalli (2009) outlined that when there is lack of senior management support, there is likely some resistance. Efforts must be made by the organisation to sit with managers at all levels to highlight the importance of senior management in curbing the resistance that is being experienced. If possible, organisations must get senior managers to be the champions of SailPoint IIQ access reviews so that they can encourage the managers under them to perform access reviews.

- **User-friendliness**

The efforts of sitting down with some managers to look at the opportunities on how the user interface can be made more intuitive must be made.

- **Managers being the wrong audience of some access reviews.**

Organisations must make efforts for looking into which access is more appropriate to be reviewed by managers, and which access is more appropriate to be reviewed by other people, such as resource owners.

- **Inexistence of consequence system**

The efforts of introducing measurable job performance indicators that will measure the managers' completion of access reviews must be made so that managers can start seeing performing access reviews as part of their job functions. Consequently, if managers are not performing access reviews, they can get a lower rating during their performance reviews.

- **The inexistence of access review training specifically for managers.**

Efforts to introduce access review training for managers must be made. Friedman (2018) outlined that continuous training is important when dealing with an IGA solution.

6.6.2 Future research

While this study aimed to examine and explain why bank managers resist an access review component of SailPoint IIQ, the description provides future researchers with a reference point when they want to research a similar subject. It also provides future researchers with a description of the challenges faced with the access review component of an IGA system. The results of this study provide researchers with an opportunity to conduct studies on:

- The applicability of the updated conceptual framework in different contexts where an IGA system is used for performing access reviews.
- The importance of 'Perception' when studying resistance of an Access Review component of an IGA System.

6.7 Limitations

The study achieved its primary objective, which is to explain why bank managers resist the access review component of SailPoint IIQ. However, on the 15th of March 2020, the South African president, Mr Cyril Ramaphosa, declared a national state of disaster, resulting in the suspension of most face-to-face activities. As a result, the researcher was not allowed to conduct face-to-face interviews, which led to conducting interviews electronically. Electronic interviews had their technical limitations, which were mostly related to network issues, and due to the research methodology that the researcher followed, the researcher could not re-interview some participants. The researcher found himself in a situation where he had to let go of some interviews because the audio recording was not audible due to network reception at participants' areas.

6.8 Limitations of the Conceptual Framework

Traditionally, the framework by Lapointe and Rivard (2005) has been applied in longitudinal studies (Lapointe & Rivard, 2005; Rivard & Lapointe, 2012; Selander & Henfridsson, 2012), where there were different episodes that were studied and the uncovering of how resistance behaviours changes over time after responses by the project teams have altered initial conditions and objects of resistance. This research applied the framework cross-sectionally, and as a result the study cannot explain how the resistance changes over-time, for example, if the researcher could get results after the user interface is made more intuitive, would the participants have similar perceptions about resistance of the access review component of SailPoint IIQ at ABC Bank?

Overall, what makes bank managers to not perform access reviews on SailPoint IIQ is the perception that managers develop because of an interplay between the initial conditions and the object of resistance. Moreover, the existence of the factors[7] that influence managers to not perform access reviews is also the reason behind why bank managers do not perform access reviews on SailPoint IIQ.

[7] Initial conditions related to the system itself

Adeleke, A. (2016). *Investigating user resistance to information systems (IS) implementation*. Colorado Technical University.

Ali, M., Zhou, L., Miller, L., & Ieromonachou, P. (2016). User resistance in IT: A literature review. *International Journal of Information Management*, *36*(1), 35–43.

Andress, J. (2011). Authorization and Access Control. In *The Basics of Information Security*.

Angraini, Alias, R. A., & Okfalisa. (2019). Information Security Policy Compliance: Systematic Literature Review. *Procedia Computer Science*, *161*, 1216–1224.

Anney, V. N. (2014). *Ensuring the Quality of the Findings of Qualitative Research: Looking at Trustworthiness Criteria*.

Atyam, S. B. (2010). Effectiveness of Security Control Risk Assessments for Enterprises: Assess on the Business Perspective of Security Risks. *Information Security Journal: A Global Perspective*, *19*(6), 343–350.

Bagayogo, F., Beaudry, A., & Lapointe, L. (2013). Impacts of IT Acceptance and Resistance Behaviors: A Novel Framework. *Proceedings of the 34th International Conference on Information Systems*.

Beigi, S. (2015). Organizational Silence A Dangerous Phenomenon in the Way of the Organizational. *International Journal of Basic Sciences & Applied Research*, *3*(1), 300–306.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Bhattacherjee, A. (2012). Social Science Research: principles, methods, and practices. In *Textbooks collection*.

Bloomberg, B., Cooper, D. R., & Schindler, P. S. (2011). *Business research methods* (Third Euro). Mc Graw Hill Education.

Bradford, M., & Florin, J. (2003). Examining the role of innovation diffusion factors on the implementation success of enterprise resource planning systems. *International Journal of Accounting Information Systems*. https://doi.org/10.1016/S1467-0895(03)00026-5

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bredmar, K. (2017). Change management. In *The Routledge Companion to Accounting Information Systems*. https://doi.org/10.4324/9781315647210

Burnes, B. (2015). Understanding Resistance to Change – Building on Coch and French. *Journal of Change Management*, *15*(2), 92–116.

Cameron, A., & Grewe, O. (2020). An Overview of the Digital Identity Lifecycle. *IDPro Body of Knowledge*, *1*(3).

Charness, N., & Boot, W. R. (2015). Technology, Gaming, and Social Networking. In *Handbook of the Psychology of Aging: Eighth Edition* (pp. 389–407). Elsevier Inc. https://doi.org/10.1016/B978-0-12-411469-2.00020-0

Coetsee, L. M. A. (1993). A practical model for the management of resistance to change: An analysis of political resistance in south africa. *International Journal of Public Administration*, *16*(11), 1815–1837.

Cooper, D. R., & Schindler, P. S. (2014). *Business research methods, Twelfth Edition*.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372.

Davey, S. (2016). *SailPoint celebrates 10 years, record profitability, growth beyond $100m annual revenue*. ITWeb. https://www.itweb.co.za/content/KrxP3jMBKVDqA2ye

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/249008

de Villiers, D., Govender, D., & Madumo, E. (2020). *Banking Laws and Regulations | South Africa | GLI*. https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/south-africa

Del Val, M. P., & Fuentes, C. M. (2003). Resistance to change: a literature review and empirical study. *Management Decision*, *41*(2), 148–155.

Denolf, J. M., Trienekens, J. H., Wognum, P. M. (Nel), van der Vorst, J. G. A. J., & Omta, S. W. F. (Onno). (2015). Towards a framework of critical success factors for implementing supply chain information systems. *Computers in Industry*, *68*, 16–26. https://doi.org/https://doi.org/10.1016/j.compind.2014.12.012

Dent, E. B., & Goldberg, S. G. (1999). Challenging resistance to change. *Journal of Applied Behavioral Science*.

Enns, H. G., Huff, S. L., & Higgins, C. A. (2003). CIO Lateral Influence Behaviors: Gaining Peers' Commitment to Strategic Information Systems. *MIS Quarterly*. https://doi.org/10.2307/30036522

Erwin, D. G., & Garman, A. N. (2010). Resistance to organizational change: Linking research and practice. *Leadership and Organization Development Journal*, *31*(1), 39–56. https://doi.org/10.1108/01437731011010371

Fernandes, O. J., Portugal, L. C., Alves, R. C., Campagnoli, R. R., Mocaiber, I., David, I. P., Erthal, F. C., Volchan, E., de Oliveira, L., & Pereira, M. G. (2013). How you perceive threat determines your behavior. *Frontiers in Human Neuroscience*, *7*, 632.

Fin24. (2016). *R30m fine: Sarb nails 5 banks after money-laundering probe*. https://www.news24.com/fin24/economy/r30m-fine-sarb-nails-5-banks-after-money-laundering-probe-20160808

Ford, J. D., & Ford, L. W. (2009). Decoding Resistance to Change. *Harvard Business Review*, *87*(4), 99–103.

Friedman, J. (2018). The Ultimate Guide to Identity Governance. *CyberEdge Group*, 1–48.

Fugate, M., Prussia, G. E., & Kinicki, A. J. (2010). Managing Employee Withdrawal During Organizational Change. *Journal of Management*, *38*(3), 890–914. https://doi.org/10.1177/0149206309352881

Gaehtgens, F., Kampman, K., Data, A., Teixeira, H., & Collinson, D. (2019). *Magic Quadrant for Identity Governance and Administration*. https://www.gartner.com/doc/reprints?id=1-1QWSGZQK&ct=191009&st=sb

Garcia, M. L., & Bray, O. H. (1997). *Fundamentals of technology roadmapping*.

Haddara, M., & Moen, H. (2017). User resistance in ERP implementations: A literature review. *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2017.11.111

Hamon, P., Seguin, M., Perrier, X., & Glaszmann, J. C. (2003). *Genetic diversity of cultivated tropical plants*.

Harkness, W. L., Kettinger, W. J., & Segars, A. H. (1996). Sustaining Process Improvement and Innovation in the Information Services Function: Lessons Learned at the Bose Corporation. *MIS Quarterly*, *20*(3), 349–368. https://doi.org/10.2307/249661

Hirschheim, R., & Newman, M. (1988). Information Systems and User Resistance: Theory and Practice. *The Computer Journal*, *31*(5), 398–408.

Hunter, M. G. (2005). Qualitative research in information systems: consideration of selected theories. In *Information Systems Foundations: Constructing and Criticising*.

Identity Management Institute. (2019). *Access Certification*. https://www.identitymanagementinstitute.org/access-certification/

ISO 27001. (2013). *Information technology - Security techniques - Information security management systems - Requirements*.

ISO 27002. (2013). *Information technology - Security techniques - Code of practice for information security controls*.

Joshi, K. (1991). A Model of Users' Perspective on Change: The Case of Information Systems Technology Implementation. *MIS Quarterly*, *15*(2), 229–242.

Juergens, H. F. (1977). Attributes of Information System Development. *MIS Quarterly*, *1*(2), 31–41. https://doi.org/10.2307/249166

Kim, & Kankanhalli. (2009). Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective. *MIS Quarterly*, *33*(3), 567–582.

King, N. (2004). Using interviews in qualitative research. In C. Cassell & G. Symon (Eds.), *Essential Guide to Qualitative Methods in Organizational Research* (pp. 11–22). Sage. http://eprints.hud.ac.uk/id/eprint/1792/

Klaus, T., & Blanton, J. E. (2010). User resistance determinants and the

psychological contract in enterprise system implementations. *European Journal of Information Systems*, *19*(6), 625–636.

Kouns, B. L., & Kouns, J. (2011). THE INFORMATION SECURITY MANAGEMENT SYSTEM. In *The Chief Information Security Officer: Insights, tools and survival skills* (pp. 45–52). IT Governance Publishing.

Landaeta, R. E., Mun, J. H., Rabadi, G., & Levin, D. (2008). Identifying sources of resistance to change in healthcare. *International Journal of Healthcare Technology and Management*, *9*(1), 74–96. https://doi.org/10.1504/ijhtm.2008.016849

Lapointe, & Rivard. (2005). A Multilevel Model of Resistance to Information Technology Implementation. *MIS Quarterly*, *29*(3), 461–491.

Laumer, S., Eckhardt, A., & Weitzel, T. (2016). *Work routines as an object of resistance during information systems implementations : theoretical foundation and empirical evidence*. *25*(4), 317–343. https://doi.org/10.1057/ejis.2016.1

Li, D., Huang, W. W., Luftman, J., & Sha, W. (2011). Key Issues in Information Systems Management. *Journal of Global Information Management*. https://doi.org/10.4018/jgim.2010100102

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. CA: Sage.

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, *1986*(30), 73–84.

Lopes, I., & Oliveira, P. (2016). The security policy application process: Action research. *Advances in Intelligent Systems and Computing*, *445*, 353–362.

Lopes, I., Pereira, J., & Oliveira, P. (2017). Definition of information systems security policies. *Advances in Intelligent Systems and Computing*, *571*, 225–234.

Luftman, J., Zadeh, H. S., Derksen, B., Santana, M., Rigoni, E. H., & Huang, Z. D. (2013). Key information technology and management issues 2012-2013: An international study. *Journal of Information Technology*.

Marakas, G. M., & Homik, S. (1996). Passive resistance misuse: Overt support and covert recalcitrance in IS implementation. *European Journal of Information*

Systems.

Markus, M. L. (1983). Power , Politics , and MIS Implementation. *Communications of the ACM*, *26*(6), 430–444.

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37–46. https://doi.org/10.1016/j.chb.2018.10.031

Meyer, V., & Van Schalkwyk, L. (2018). *ACCESS GOVERNANCE - THE NEDBANK JOURNEY*. https://www.idjohannesburg.co.za/assets/presentations/id_JHB Nedbank Presentation_.pdf

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *41*(1), 285–311. https://misq.org/toward-a-unified-model-of-information-security-policy-compliance.html

Morris, T., & Wood, S. (1991). Testing the survey method: Continuity and change in british industrial relations. *Work Employment & Society*, *5*(2), 259–282. https://doi.org/10.1177/0950017091005002007

Moyo, M. (2019). *Standard Bank Group - Identity Access Management at Scale*. https://www.idjohannesburg.co.za/assets/presentations/8. Melusi - Standard Bank - Identity Governance.pdf

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly Discovery*.

Neira, B. (2020). Securing Corporate Resources Using Identity Governance. *ProQuest LLC*, *May*.

Newman, M., & Robey, D. (1992). A Social Process Model of User-Analyst Relationships. *MIS Quarterly*, *16*(2), 249–226.

Oates, B. J. (2006). Researching Information Systems and Computing. *Inorganic Chemistry*.

Omarjee, L. (2017). *SARB fined banks R46.5m in 2016 for control weaknesses - report*. Fin24. https://www.news24.com/fin24/companies/financial-services/sarb-fined-banks-r465m-in-2016-for-control-weaknesses-report-20170526

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*.

Pandey, S., & Patnaik, S. (2014). ESTABLISHING RELIABILITY AND VALIDITY IN QUALITATIVE INQUIRY: A CRITICAL EXAMINATION. *Jharkhand Journal of Development and Management Studies*, *12*, 5743–5753.

Peltier, T. R., & Peltier, J. (2016). Complete Guide to CISM Certification. In *Complete Guide to CISM Certification*. Auerbach Publications.

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology*, *52*(2), 137.

Ramluckan, T., & Van Niekerk, B. (2014). Security Requirements for Cloud Computing in Crisis Management. *Source: Journal of Information Warfare*, *13*(1), 33–46.

Rigon, E. A., Westphall, C. M., Dos Santos, D. R., & Westphall, C. B. (2014). A cyclical evaluation model of information security maturity. *Information Management and Computer Security*, *22*(3), 265–278.

Rivard, S., & Lapointe, L. (2012). Information Technology Implementers' Reponses To User Resistance: Nature and Effects. *MIS Quarterly*, *36*(3), 897–920.

Robson, C. (2002). Real world research. In *Blackwell Publishing*. https://doi.org/10.1016/j.jclinepi.2010.08.001

Rogers, E. M. (1995). Diffusions of Innovations. In *Diffusions of Innovations*.

Rouhani, S., Pourheidari, V., & Deters, R. (2018). Physical Access Control Management System Based on Permissioned Blockchain. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1078–1083. https://doi.org/10.1109/Cybermatics_2018.2018.00198

Rousseau, D. M. (1989). Psychological and implied contracts in organizations. *Employee Responsibilities and Rights Journal*. https://doi.org/10.1007/BF01384942

Rumelt, R. P. (1995). Inertia and transformation. In *Resource-based and evolutionary theories of the firm: Towards a synthesis* (pp. 101–132). Springer.

Sabi, H. M., Mlay, S. V, Tsuma, C. K., & Bang, H. N. (2015). Conceptualizing User Preference and Trust in Western Designed Banking Software Systems in Developing Countries. *Journal of Internet Banking and Commerce*, *5*(1), 1–24.

SailPoint. (2018). *A Complete and Open Identity Governance Solution*.

SailPoint. (2019). *IdentityIQ: Inteligent Cloud Identity Platform, Software Solution*. https://docs.sailpoint.com/pdf/?file=https://docs.sailpoint.com/wp-content/uploads/SailPoint-IdentityIQ-Brochure.pdf

Sakala, L. C. (2019). Resistance to the implementation of learning management systems by lecturers in higher education in a developing country context.

Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The Science of Training and Development in Organizations: What Matters in Practice. *Psychological Science in the Public Interest*, *13*(2), 74–101. http://www.jstor.org/stable/23484697

Saunders, M., Lewis, P., & Thornhill, A. (2009a). Formulating the research design. In *Research Methods for Business Students Fifth edition*. https://doi.org/10.1017/CBO9781107415324.004

Saunders, M., Lewis, P., & Thornhill, A. (2009b). Selecting samples. In *Research Methods for Business Students Fifth edition*. https://doi.org/10.1017/CBO9781107415324.004

Seidel, J. V. (1998). Qualitative Data Analysis. In *Ethnograph v5*.

Selander, L., & Henfridsson, O. (2012). Cynicism as user resistance in IT implementation. *Information Security Journal*, *22*(4), 289–312.

Senn, J. A. (1978). Essential Principles of Information Systems Development. *MIS Quarterly*, *2*(2), 17–27.

Seo, D., Boonstra, A., & Offenbeek, M. (2011). Managing IS adoption in ambivalent groups. *Communications of the ACM*, *54*(11), 68–73.

Shabani, M., Dyke, S. O. M., Joly, Y., & Borry, P. (2015). Controlled Access under Review: Improving the Governance of Genomic Data Access. In *PLoS Biology*.

Sikhakhane, J. (2016). *South African Reserve Bank imposes administrative sanctions on two banks*. https://www.resbank.co.za/publications/detail-item-view/pages/publications.aspx?sarbweb=3b6aa07d-92ab-441f-b7bf-bb7dfb1bedb4&sarblist=21b5222e-7125-4e55-bb65-56fd3333371e&sarbitem=7604

Sikora, A., Margalef, T., & Jorba, J. (2015). Online root-cause performance analysis of parallel applications. *Parallel Computing*, *48*, 81–107. https://doi.org/https://doi.org/10.1016/j.parco.2015.05.003

Smedinghoff, T. J. (2008). The Role of Standards. In *Information Security Law Book Subtitle: The Emerging Standard for Corporate Compliance* (pp. 120–137). IT Governance Publishing.

Smith, N. C., Drumwright, M. E., & Gentile, M. C. (2010). The New Marketing Myopia. *Journal of Public Policy & Marketing*, *29*(1), 4–11. https://doi.org/10.2139/ssrn.1336886

Steyn, M., & Espag, D. (2019). *IDENTITY GOVERNANCE AND ADMINISTRATION - Identity at the Speed of Cloud*. https://www.idjohannesburg.co.za/assets/presentations/4. Michael - Old Mutual IGA SailPoint Presentation Oct2019.pdf

van Dijk, R., & van Dick, R. (2009). Navigating Organizational Change: Change Leaders, Employee Resistance and Work-based Identities. *Journal of Change Management*, *9*(2), 143–163. https://doi.org/10.1080/14697010902879087

Vrhovec, S. L. R. (2016). Responding to stakeholders' resistance to change in software projects - A literature review. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings*. https://doi.org/10.1109/MIPRO.2016.7522314

Waddell, D., & Sohal, A. S. (1998). Resistance : a constructive tool for change management. *Management Decision*, *36*(8), 543–548.

Walsham, G. (2017). ICT4D research: reflections on history and future agenda. *Information Technology for Development*. https://doi.org/10.1080/02681102.2016.1246406

Watson, J. (2011). Resistance is futile? Exploring the potential of motivational

interviewing. *Journal of Social Work Practice*, *25*(4), 465–479. https://doi.org/10.1080/02650533.2011.626653

Xia, W., & Lee, G. (2005). Complexity of information systems development projects: Conceptualization and measurement development. *Journal of Management Information Systems*, *22*(1), 45–83.

Yin, R. K. (1994). Case study research: design and methods. *Thousand Oaks, CA*.

Yin, R. K. (2003). Case Study Research, Design ad Method. In *Qualitative Research*. https://doi.org/10.3917/rsi.103.0020

Zhang, C. N., & Yang. (2003). Integrating object oriented role-based access control model with mandatory access control principles. In *The Journal of Computer Information Systems; Spring* (Vol. 43).

Zhao, X., & Johnson, M. E. (2010). Access governance: Flexibility with escalation and audit. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–13.

Appendix A: Interview Protocol

The primary research question is ‘Why do bank managers resist the use of the access certification component of SailPoint IIQ?’

1. General Questions

- In your understanding, what is access review, certification, recertification?
- What do you think the use of SailPoint IIQ is in the bank? Please explain.

2. Main Questions

Variable	**Research Question (Guiding Question)**	**Possible questions**
Resistance behaviour	What are the bank managers’ behaviours towards the access review component of SailPoint IIQ?	There are four common behaviours of resistance as per Coetsee, (1993): ***Apathy*** *– Meaning some managers are still indifferent about performing access reviews on SailPoint IIQ.* ***Passive resistance*** *– Meaning some managers give excuses as to why they do not perform access reviews on SailPoint IIQ.* ***Active resistance*** *- Meaning some managers go around trying to convince other managers not to perform access reviews on SailPoint IIQ.*

Variable	Research Question (Guiding Question)	Possible questions
		Aggressive resistance *– They some managers threaten managers that perform access reviews on SailPoint IIQ.* How do you believe managers resist the access review component of *SailPoint* IIQ? Why?
Perception	Why do bank managers resist the use of the access certification component of SailPoint IIQ?	*Previous research stated that some users do not use a system or its functionalities because they 1) believe that it does not add value towards their job performance, 2) they find it difficult to use, 3) believe the system is worse off relative to other systems (Bradford & Florin, 2003; Charness & Boot, 2015; Davis, 1989; Rogers, 1995) 4) think that there are no consequences of not using the system, and many more perceptions (Merhi & Ahluwalia, 2019).* What do you think are some managers' perceptions or views about the access review component of SailPoint IIQ that might lead them to not performing access reviews on it?
Initial Conditions	What influence bank managers not to perform access reviews?	*Some previous studies stated that things such as for example, past bad experiences, knowledge, denial, top management inaction, and many more*

Variable	Research Question (Guiding Question)	Possible questions
		factors do influence people not to use or to resist a system. Del Val & Fuentes (2003). What do you believe are the factors influencing managers not to perform access reviews on SailPoint IIQ?
		Based on what you just said, what would you say makes the managers not to perform access reviews on SailPoint IIQ?
Object of resistance	What do bank managers resist?	What do you think bank managers are resisting?

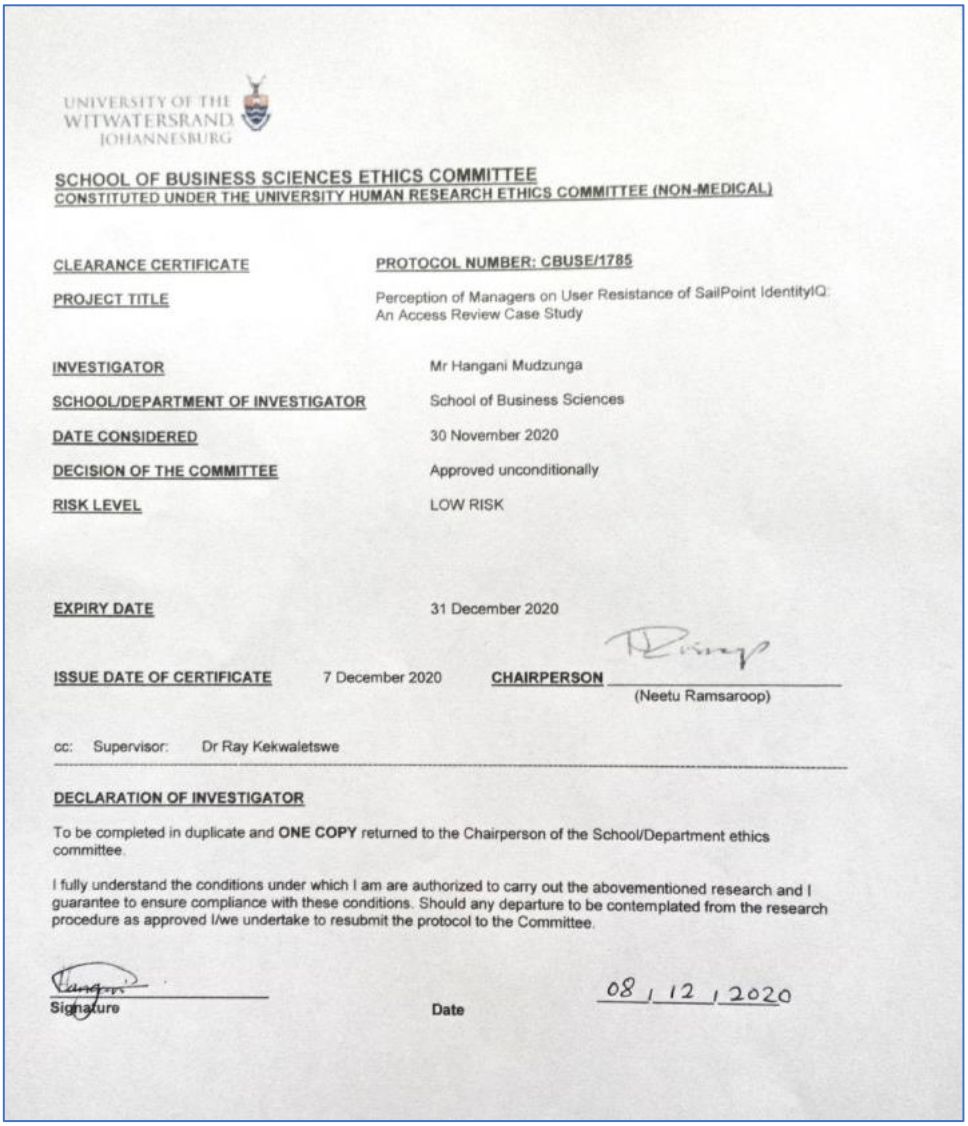
Senior Managers and Executive Managers Questions

1. Have you previously received an escalation from SailPoint IIQ stating that one of your Subordinates have not completed their reviews on time? If yes, please explain the reasons behind them not completing an access review or not doing so in time.

Personal questions

2. Have you previously not completed an access review on SailPoint IIQ or got escalated for not completing an access review on time? If yes, please explain the reasons behind not completing an access review or not doing so in time.

Appendix B: Ethics Clearance Certificate



UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG

SCHOOL OF BUSINESS SCIENCES ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE	**PROTOCOL NUMBER: CBUSE/1785**
PROJECT TITLE	Perception of Managers on User Resistance of SailPoint IdentityIQ: An Access Review Case Study
INVESTIGATOR	Mr Hangani Mudzunga
SCHOOL/DEPARTMENT OF INVESTIGATOR	School of Business Sciences
DATE CONSIDERED	30 November 2020
DECISION OF THE COMMITTEE	Approved unconditionally
RISK LEVEL	LOW RISK
EXPIRY DATE	31 December 2020

ISSUE DATE OF CERTIFICATE 7 December 2020 **CHAIRPERSON** _____
(Neetu Ramsaroop)

cc: Supervisor: Dr Ray Kekwaletswe

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ 08 / 12 / 2020
Signature **Date**

Appendix C: Consent Form

Research Participation Consent Form

Title of project Perception of Managers on User Resistance of SailPoint IdentityIQ: An Access Review Case Study

Name of researcher Mr Hangani Mudzunga

I ..... agree to participate in this research project. The research has been explained to me and I understand what my participation will involve.

	Options	
	YES	NO
I agree that my participation will remain anonymous		
I agree that the researcher may use anonymous quotes in his/her research report		
I agree that the interview may be audio recorded		
It has been explained to me that I can withdraw from the interview at any given time		
It has been explained to me that the researcher is not getting compensated for conducting this research.		
I understand that there will not be any reward for participating in this project		

..... (signature)

..... (name of participant)

..... (date)

University of the Witwatersrand,
1 Jan Smuts Avenue,
Braamfontein,
2000
Johannesburg,
South Africa

Appendix D: Participant Sheet

Participant Information Sheet

Dear Sir/Madam

My name is Hangani Mudzunga and I am a Masters student in the department of Information Systems at Wits University in Johannesburg. As part of my studies I have to undertake a research project, and I am investigating Perception of Managers on User Resistance of SailPoint IdentityIQ (commonly known as [redacted] in [redacted]). The aim of this research project is to find out why bank managers resist using the access review component of SailPoint IIQ.

As part of this project I would like to invite you to take part in an interview. The interview will be once-off and it will take around 30 – 60 minutes. With your permission, I would also like to record the interview.

You will not receive any direct benefits from participating in this study, and there are no disadvantages or penalties for not participating. You may withdraw at any time or not answer any question if you do not want to. The interview will be completely confidential and anonymous as I will not be asking for your name or any identifying information, and the information you give to me will be held securely and not disclosed to anyone else. I will be using a pseudonym (false name) to represent your participation, in my final research report. If you experience any distress or discomfort, we will stop the interview or resume another time.

If you have any questions afterwards about this research, feel free to contact me on the details listed below. This study will be written up as a research report and If you wish to receive a summary of this report, I will be happy to send it to you upon request. If you have any queries, concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (non-medical), telephone + 27(0)11 717 1408, email , Shaun.Schoeman@wits.ac.za

Yours sincerely,
Hangani Mudzunga

Researcher details: Mr Hangani Mudzunga, 476167@students.wits.ac.za, +27(0)79 746 6549
Supervisor details: Dr. Ray Kekwaletswe, Ray.Kekwaletswe@wits.ac.za, +27(0)11 717 8146

University of the Witwatersrand,
1 Jan Smuts Avenue,
Braamfontein,
2000
Johannesburg,
South Africa