
# An integrated approach for information security compliance in a financial services organisation

by

Mohammed Reza Desai

Dissertation submitted in fulfilment of the requirements for the degree

**Master of Technology: Information Technology**

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

**Supervisor:** Dr AC de la Harpe

Cape Town

January 2016

**Declaration**

I, Mohammed Reza Desai here, declare that the contents of this dissertation represent my own unaided work, and that the dissertation has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology

…….  ……

Signature  Date

**Abstract**

The aim of this research is to identify and explore the factors affecting information security compliance of information security policies and regulations, in a financial services organisation. The organisation has to comply with information security regulations and legislations by righteousness of its operations in light of the fact that any wrong doing together with misuse of data, are continually expanding. Corporate embarrassments comes about due to rupture of security, results in expanded thoughtfulness regarding corporate consistency. Legislature and policies have been set up to counter information security issues. This legislature and policies are not adequately addressing the compliance issues that arise, but are needed within organisations. Compliance targets are not met due to inconsistent guidelines that turns out to be significant in diminishing the financial position, reputation and security of information.

This research further aims to explore whether employees comply with laws and regulations regarding information in an organisation. This is done in order to confirm whether governance and human factors play any significant part in compliance. The research is an exploratory study and specifically analyses the governance function and which stakeholders influence its operations in information compliance. The research investigates certain questions on organisational culture and the human factor, do influence employee's compliance to laws and regulations. The objectives of the research are to investigate which factors, and how such factors influence compliance of information security policies and compliance with the goal of designing an integrated framework to assist in counteracting these findings. The research is underpinned by the Neo-institutional theory, Agency Theory and Rational choice theory. The Denison organisational cultural model and a framework proposed by von Solms are used as lenses to interpret the data of the research.

The thesis outlines a qualitative research on the topic of information security compliance within a financial services organisation in Cape Town, South Africa. Focusing on literature and some compliance theories, the ways are examined in which legal compliance and information security departments work together when protecting financial assets. The thesis proposes an integrated framework by

including the human factor, when complying with information security compliance objectives. The research uses a qualitative approach by means of a case study, that is used to evaluate whether this approach provides a superior means of resolving the legal-technological gap. An interpretivist stance from a subjectivist ontology guides the research. The research approach is inductive and a case study as a research strategy. Data is collected using 21 interviews and an interview guide used to guide the interviewer through the process and consists of semi-structured questions. Data is analysed by means of summarising, categorising and thematic analysis. A proposed integrated framework is developed by incorporating findings of the research into Neo-institutional theory, The Denison organisational cultural model and the von Solms framework.

**Keywords**

Information security, information security compliance, information security framework, organisational culture, governance, legislature, information security culture, integrated IT framework, financial services

**Table of Contents**

Glossary ..... 1

1. Introduction ..... 4

1.1 Background ..... 4

1.2 Research Problem ..... 5

1.3 Research Aims ..... 8

1.4 Research methodology ..... 8

1.4.1 Research philosophy ..... 8

1.4.1.1 Ontology ..... 8

1.4.1.2 Epistemology ..... 9

1.4.2 Research approach ..... 9

1.4.2.1 Inductive ..... 9

1.4.3 Research strategy ..... 9

1.4.3.1 Sampling ..... 10

1.4.3.2 Unit of analysis ..... 10

1.4.3.3 Data collection ..... 10

1.4.3.4 Data analysis ..... 10

1.5 Assumptions ..... 10

1.6 Delineation ..... 11

1.7 Ethics ..... 11

1.8 Summary ..... 11

2. Literature Review ..... 13

2.1 Introduction ..... 13

2.2 Information Security and policies ..... 14

2.2.1 Models and approaches ..... 16

2.3 Culture ..... 20

2.3.1 Organisational culture ..... 20

2.3.2 Information security culture ..... 22
2.3.3 Information Security Policies ..... 24
2.4 Governance and Compliance ..... 25
2.5 Legislation and Regulations ..... 30
2.6 Theories, Models and Frameworks ..... 34
2.6.1 Neo-institutional theory ..... 35
2.6.2 Agency Theory ..... 37
2.6.3 Rational Choice Theory ..... 38
2.6.4 Elaboration likelihood Model ..... 39
2.7 Organisational culture model ..... 40
2.8 A Governance Framework for Information Security ..... 42
2.9 Summary of compliance theories ..... 45
2.10 Proposed Conceptual Framework ..... 46
2.11 Summary ..... 47
3. Research Methodology ..... 49
3.1 Introduction ..... 49
3.2 Research design process ..... 49
3.3 Research philosophy ..... 51
3.3.1 Ontology ..... 51
3.3.2 Epistemology ..... 52
3.4 Research Approach ..... 54
3.5 Research Strategy ..... 56
3.5.1 Unit of analysis ..... 57
3.6 Data collection ..... 58
3.7 Data Analysis ..... 59
3.8 Ethics ..... 61
3.9 Summary ..... 62

4. Findings ..... 64
4.1 Introduction ..... 64
4.2 The case ..... 64
4.3 The Findings ..... 65
4.4 Summary of the findings ..... 88
4.5 Summary ..... 96
5. Discussion and conclusions ..... 98
5.1 Introduction ..... 98
5.2 The proposed framework ..... 103
5.3 Conclusions ..... 105
5.4 Summary ..... 108
6. Recommendations, reflection and contributions ..... 109
6.1 Recommendations ..... 109
6.2 Reflection ..... 110
6.3 Contribution of Research ..... 110
6.4 Contribution to Information Technology ..... 111
6.5 Contribution to Law and Compliance ..... 111
6.6 Contribution to Organisational Culture ..... 112
6.7 Limitations of Research ..... 112
References ..... 114
Appendix 1 – Interview guide ..... 126
Appendix 2 - Summary of interview responses ..... 129
Appendix 3 - Consent letters: examples of company and participant consent ..... 145

## Glossary

**Banks Act** - Requires all banks to follow in order to provide banking services. Provides the requirements of doing business in the sector (Maphakela & Pottas, 2006:51).

**Basel Code -** To improve the soundness and stability of the international banking system by promoting: Minimum capital requirements, Supervisory review process and Market discipline (Hussein & Al-Tamimi, 2008:174).

**Coercive pressure –** as a result of an organisation that experiences institutionalised pressure from an external organisation to which they need in order to operate (Hu, Hart & Cooke, 2007:157).

**Compliance –** "relationship in which an actor behaves in accordance with the directive supported by another actor's power, and to the orientation of the subordinated actor to the power applied" (Kolkowska & Dhillon, 2013:4).

**Electronic Communications and transactions (ECT Act)** – Used to promote the facilitation and regulation of electronic communications and transactions and to prevent misuse of systems (Parliament of the Republic of South Africa, 2002).

**Financial Advisory and Intermediary Services Act (FAIS)** - Protects the consumers of financial products and services and provides regulations to govern it (Financial Advisory and Intermediary Act, 2002).

**Financial Intelligence Centre Act (FICA) -** To establish a Financial Intelligence Centre and Anti Money Laundry Council in order to fight money laundering and terrorism activities by preventing false identification (Parliament of the Republic of South Africa, 2001).

**Graham Leach Bibley -** Provides a financial structure on how to protect financial information (Maphakela & Pottas, 2006:54).

**Information security -** "the preservation of confidentiality, integrity and availability of information" (Dimitriadis, 2011:43).

**Information security Culture -** all socio-cultural measures that support technical security measures and that limits its focus to both sub-dimensional information and the belief that information security is a technical problem (Ruighaver, Maynard & Chang, 2007:56).

**Information security governance -** consists of the management of commitment and leadership, the organisational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms which all works together to ensure integrity (von Solms, 2006:444).

**King Code -** "The King Report applies to all companies listed on the board of the JSE, such as large public entities, banks and other financial and insurance entities. The purpose of the King Report is to promote the highest standard of corporate governance for companies" (Maphakela & Pottas, 2006:49).

**Mimetic pressure –** comes about as a result of organisations needing to model themselves to copy other organisations in the environment they operate in to be successful (Hu *et al*., 2007:157).

**Normative pressure –** appropriate ways to act in the organisation with regard to culture and profession (Hu *et al.*, 2007:157).

**Policy –** is a set of procedures that are used to be a guideline for good practice (Thomson & Van Niekerk, 2012:44).

**Protection of Personal Information Act (POPI) -** Promoting minimum requirements for the processing of information. Securing the integrity of personal information in its possession or under its control by taking prescribed measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information (Parliament of the Republic of South Africa, 2013).

**Sarbanes Oxley (SOX) –** Explicitly certifies that the organisation will accept responsibility to establish and maintain adequate financial reporting and appropriate internal control systems (Gordon, Loeb, Lucyshyn & Sohail, 2006:504).

**List of Tables**

Table 1.1: Research Questions, sub-research questions, methods and objectives of the questions ……..…6
Table 2.2: International and national legislation affecting the organisation.……33
Table 2.3: Summary of the compliance theories and models…….....45
Table 4.1: Summary of findings……..…88
Table 4.2: Linkage between theory, framework constructs, factors affecting information security, interview questions, findings and themes……...95

**List of Figures**

Figure 2.1 Intrinsic and extrinsic motivators in information security behaviours (Herath & Rao, 2009a:156)……..…18
Figure 2.2: Daniel Denison's organisational culture model (Denison, Haanland & Goelzer, 2004:101)……42
Figure 2.3: A Governance Framework for Information Security (Posthumus & von Solms, 2004:645)……43
Figure 2.4: The proposed conceptual framework……47
Figure 5.1: Proposed Integrated Framework for Information Security Compliance……105

**Abbreviations**

BOD – Board of Directors
CO – Control Objective
COBIT – Control Objectives for Information and Related Technology
CPUT – Cape Peninsula University of Technology
DCO – Detailed Control Objective
ELM – Elaboration Likelihood Model
IT – Information Techology
ITIL – Information Technology Infrastructure Library

# 1. Introduction

## 1.1 Background

The effect of information security breaches could manifest in organisations potentially making substantial financial losses (Da Veiga & Eloff, 2010). Organisations that store information such as customer data, bank account details, financial and strategic information, could put their business at risk, if such information falls into the wrong hands. The extensive use of information technology (IT) especially, in the business environment, requires that organisational management be diligent in controlling the use and risk of IT.

In order to protect consumers, procedures, compliance and governance rules are put in place within institutions. It is found that many of these rules are drawn up by the legal fraternity, and implemented through IT. The interconnectedness of legal counsel and IT, creates a gap in understanding how information security breaches actually occur. Knowledge of these gaps are important aspects for the industry in which the organisation operates (Luthy & Forcht, 2006).

Governance of information, information security and information security compliance approaches are well documented (Kolkowska & Dhillon, 2013; Freeman, 2007; von Solms, 2006, 2001; von Solms & von Solms, 2004; Vroom & von Solms, 2004). However, according to Racz, Weippl and Seufert (2010), there is a lack of research on the integrated approaches towards IT governance and compliance. For example, people who entrust their financial assets to financial institutions,mneed to trust such institutions for the safekeeping of their assets.

The research case study used is an asset management organisation in Cape Town, South Africa. In this organisation, there are two departments which are responsible for information compliance namely, the Technology and the Compliance departments. They work together to keep the information of the organisation safe and secure. However, there is a gap between the processes of the Technology and Compliance departments as the human factor such as organisation culture is not properly addressed in the department's policies.

The departments have no control over employees leaking information intentionally or unintentionally. Another raising concern is the tracking of employees to determine whether the employees are in fact complying with information laws and regulations. The organisation only addresses these issues once security breaches occur. This could potentially lead to damaging consequences in the near future. There is a need to comply to laws and regulations as the financial services industry is highly regulated.

The organisation is aware of the eagerness of the Financial Services Board to expose their failure to meet requirements. Therefore, the motivation to comply is based on fear, rather than on a proactive desire to protect the company's most important assets. This points to an entrenched organisational culture that lacks cohesion, buy-in from individuals and other important aspects (Thomson & Van Niekerk, 2012).

Organisational environments are known for power struggles between people in specific departments and the processes that are designed to keep the organisation in compliance with regulatory requirements (Veiga & Martins, 2015).The reality of the inability to understand this relationship by stakeholders leads to a lack of compliance to laws and policies (Kolkowska & Dhillon, 2013). The number of regulations handed down from authorities also poses difficulties for organisations to demonstrate that information security is managed at a satisfactory level. The cost of complying with regulations is high in terms of investment put towards compliance and penalties received. End user security behaviour also presents a challenge, as users have different views on how management is driving information security compliance practices (Herath & Roa, 2009a).

### 1.2 Research Problem

The importance of information security is evident after security breaches resulted in organisation financial losses (Da Veiga & Eloff, 2010). This is supported by Sommestad, Hallberg, Lundholm and Bengtsson (2013) stating that information security is a growing concern in organisations and there are many internal and

external security threats that relate to information assets. As and when security threats or breaches occur, companies initiate and implement compliance objectives in an ad hoc way. The result is an approach that lacks continuity and consistency (Ciarlone, 2006). In the case of information security compliance, these approaches lead to situations in which employees neither utilize, nor truly understand these approaches, because they can be at best be, disjointed and at worst, contradictory (Thomson & Van Niekerk, 2012). Governance of information, information security and information security compliance approaches are well documented (Kolkowska & Dhillon, 2013; Freeman, 2007; von Solms, 2006, 2001; von Solms & von Solms, 2004; Vroom & von Solms, 2004). However, according to Racz *et al.* (2010), there is a lack of research focused on the integrated approaches towards IT governance and information security compliance. Marnewick and Labuschagne conducted a survey and reported that South Africa's financial services organisations, generally define these practices poorly and unclearly (Marnewick & Labuschagne, 2011). Furthermore, the research is fragmented and important aspects such as, organisational culture and human factors, are largely excluded in governance frameworks and information security practices (Veiga & Martins, 2015). From the above discussion, the researcher identified the research problem to be: **Fragmented compliance approaches and implementation thereof create uncertainty and failure of quality compliance within organisations and as a result may lead to reputational damage of the organisation**.

Table 1.1 depicts the research questions and research sub questions, formulated to solve the stated research problem.

Table 1.1: Research questions (RQ), sub-research questions (SRQ), methods of obtaining data and objectives of the questions.

| **RQ1** | **What factors do organisations face in order to comply with laws, regulations and information security policies?** | | |
|---|---|---|---|
| | **Question** | **Method** | **Objective** |
| **SRQ 1.1** | What are the information security compliance approaches that | Semi structured interviews | To identify what compliance approaches organisations are |

| | | | |
|---|---|---|---|
| | financial services organisations deploy? | | currently using for information security. |
| **SRQ 1.2** | What are the challenges financial services organisations face in order to comply with the regulatory body's laws and guidelines? | Semi structured interviews | To identify the challenges in order to comply with regulations and policies. |
| **RQ2** | **RQ 2: How does the information security culture influence compliance to information security policies and regulations?** | | |
| **SRQ 2.1** | How does governance influence information security compliance? | Semi structured interviews | To investigate how governance influences compliance. |
| **SRQ 2.2** | How does employee information security knowledge influence compliance? | Semi structured interviews | To investigate how human factors influences compliance. |
| **SRQ 2.3** | How does information security compliance affect employee performance? | Semi structured interviews | To determine how compliance affects employee performance. |
| **SRQ 2.4** | How do organisations manage the potential reputational damage that fragmented compliance approaches create? | Semi structured interviews | To investigate what measures or guidelines are currently in place at the organisation with reference to reputational damage. |

### 1.3 Research Aims

The aim of the research is to explore what factors are important and influence information security compliance in organisations. The main aim of the research is to explore how fragmented information security compliance approaches affect employees behaviour and awareness to comply with laws, regulations and security policies regarding information in an organisation. This is to be done in order to confirm whether aspects such as governance and human factors, play any part in information security compliance. The research is exploratory and proposes to analyse the governance function and stakeholders that influences operations in information compliance.

It is envisaged that the output of the research will add to the body of knowledge to assist future researchers in the quest to find new knowledge pertaining to information security compliance and the human aspects influencing employees.

### 1.4 Research methodology

Methodology refers to a systematic way used in problem solving. It can be referred to a science investigating on how research is to be carried out. It describes the procedures which researchers use to carry out the tasks, the research process giving descriptions, explanations and predict several phenomena (Myers, 2010).

#### 1.4.1 Research philosophy

Research philosophy is built on two main pillars namely the ontology and epistemology approaches.

##### 1.4.1.1 Ontology

Ontology is the science of the study of being. Definitions can be given to ontology as individual interpretations about what constitutes facts. It is seen as the nature of reality, which may be based on either subjectivism or objectivism (Saunders, Lewis & Thornhill, 2009). According to Saunders *et al*. (2009:110) subjectivism is about "…social phenomena which is created from the perceptions and consequent actions of those social actors concerned with their existence." On the other hand, objectivism gives the impression that the existence of social entities in reality is independent and external to the social factors which result in such existence (Saunders *et al.,* 2009).

The argument used in objectivism is the question of how or whether to establish and give proof that some specific action is either right or wrong. Objectivism can also be referred to as epistemological realism. This is a theory which gives the indication that the existence of reality is independent of the mind. The ontology for this research is based on subjectivism.

#### 1.4.1.2 Epistemology

The research is based on an interpretivist way of thinking as the research is conducted amongst people rather than objects.

### 1.4.2 Research approach

Research approach refers to the plans and procedures that were followed to conduct the research (Baxter & Jacks, 2008). Research approach entails the steps made from the broad topical assumptions within a research to the points of collecting, analysing and interpreting data. The two main approaches to research are quantitative and qualitative approach (Bryman & Bell, 2011). Quantitative approach has its links with the positivist paradigm. Data is collected and analysed in numerical forms. The analysis results in statistical calculations which are used to draw conclusions. Qualitative approach has its associations mostly with the social constructivist paradigm. This places its emphasis on reality which is socially constructed (Baxter & Jacks, 2008). The research took a qualitative approach as the research attempts to understand human behaviour and experiences.

#### 1.4.2.1 Inductive

The steps of inductive research approach start with observations made by the researcher and proceeds to the theories which are later formulated when approaching the end of the research. The researcher seeks to find patterns within the data and develop a theory from such (Baxter & Jacks, 2008). The research is inductive as it developed a framework from its findings.

### 1.4.3 Research strategy

Case study research is effective at helping to understand complex phenomenon and adds value to the previous researches on the similar matter. Case studies are more of empirical enquiries on contemporary phenomenon (Gerring, 2006). The research

is based on a case study at an asset management organisation in Cape Town, South Africa.

#### 1.4.3.1 Sampling

Sampling was chosen as this was in line with the qualitaitive approach the research adopted. The sample was selected using non-probability sampling and the researcher adopted purposive sampling in order to source qualified employees to answer the interview questions.

#### 1.4.3.2 Unit of analysis

The unit of analysis for this research study are employees with online access, network access and access to relevant information that if exposed could potentially harm the organisation in any way.

#### 1.4.3.3 Data collection

The data for this research was collected using semi structured interviews involving 21 participants, ranging from senior level to low level employees. Questions were based on a set of structured questions with the flexibility for interviewees to expand on answers (Wilson, 2014).

#### 1.4.3.4 Data analysis

The data of the research was analysed by means of i) transcribing the data, ii) reading and generating categories, themes and patterns, iii) interpreting the findings and iv) writing the report (Yin, 2013).

### 1.5 Assumptions

Financial services organisations need to comply with the laws and legislature stipulated by their countries of origin, and in particular, South Africa for this research. Information security practices are similar in the industry and the need to protect information has the same consequences as all organisations in the industry. In no way does this research attempt to generalise the findings, conclusions and recommendations.

## 1.6 Delineation

The research focusses on a case study at an asset management organisation in the financial services industry in Cape Town, South Africa. No other financial organisation such as banks and financial services providers were included. The research observes practices in one organisation and none other.

## 1.7 Ethics

To ensure ethical considerations such as honesty, objectivity, carefulness, integrity, transparency, intellectual property and confidentiality were met, it is approved by a research ethics committee at the Cape Peninsula University of Technology (CPUT), before interviews were conducted (Chapter 3. Section 3.8). It is essential to ensure that all participants anonymity and the information exchanged is executed in the correct manner and proper procedures are followed, as approved by the committee.

## 1.8 Summary

The aim of this research is to explore the factors affecting information security compliance and information security policies and regulations in a financial services organisation. The research further aims to explore whether employees comply with laws and regulations regarding information in an organisation. This is done in order to confirm whether governance and human factors play any significant part in compliance. The study is exploratory and analyses the governance function and which stakeholders, influence its operations in information security compliance. The research investigates formulated questions whether organisational culture and the human factor, do influence employee's compliance to laws and regulations. The objectives of the research are to investigate which factors and how the factors influence compliance to information security policies and compliance with the goal of designing an integrated framework to assist in counteracting these findings.

In the following Chapter 2, the review of literature is done and discusses the concepts surrounding the research problem. Chapter 3 outlines the research methodology, research approach and data analysis procedures used in the research. Chapter 4 outlines the findings from the interviews that were conducted. Chapter 5 discusses these findings and provides conclusions with a proposed framework.

Finally, Chapter 6 then provides the recommendations, reflections and limitations of the research.

# 2. Literature Review

## 2.1 Introduction

In order to find relevant literature, manual and automated search methods are used. Initially, manual searches were conducted to identify keywords, phrases and topics surrounding the research area. Research questions were derived from literature and linked back to the problem statement and aims of the study. Keywords and phrases are then used on electronic databases on the CPUT library portal. Databases accessed are; Scopus, Science Direct, Google scholar and Emerald. These four databases are found to return the best results related to the subject. The literature search covers published research over the last two decades, with a focus towards articles published as recently as possible, to provide a thorough view of literature.

This research combines technology, law and organisational analysis to enable an interdisciplinary review of literature. This chapter is structured as follows: Firstly, it provides an overview of information security (Section 2.2) and offering a summary of the current context of information security and its policies (Section 2.2.1 & 2.3.3). Furthermore, it includes literature on organisational culture (Section 2.3.1) and information security culture (Section 2.3.2), governance and compliance (Section 2.4), legislation and regulations (Section 2.5), and compliance theories and frameworks (Section 2.6) surrounding the area both, within South Africa and elsewhere. Secondly, the researcher links the compliance theories and frameworks found in literature, to the topics highlighted in an organisation related to information security, legal compliance and organisational culture.

Organisations in the twenty-first century must endeavour to remain competitive. Researchers compellingly argue that to remain competitive, organisations must be able to adapt and change (Gladwell, 2013). Organisations further need to exist as learning organisations and to maintain competitiveness, even in rapidly changing environments. Learning organisations adapt to changing contexts and adhere to sound business principles, where large and small businesses compete in the same space (Gladwell, 2013). Learning organisations maintain nimbleness by their willingness to change and adapt. This principle exists at odds to the situation where IT, security and law are three diverse fields and sometimes, known for having a

different pace of change. Due to the highly competitive environment within the financial services industry, defined nature of law and information security objectives – an integrated approach to work towards a shared goal of heightened security and quality is a necessity.

### 2.2 Information Security and policies

In this section the researcher provides an overview of information security and policies (Section 2.2). The researcher also discusses the models and approaches used in literature, given in Section 2.2.1.

Dimitriadis (2011:43) defines information security as "...the preservation of confidentiality, integrity and availability of information". Confidentiality refers to keeping the information secret whereas, integrity refers to the honesty and reliability of information. Availability of information depends on how readily information can be presented upon request.

Information security has become more vulnerable due to the increasing amount of business transactions and information processing on a daily basis (Vroom & von Solms, 2004). Information security is the protection of all activities handling information which includes, technical and non-technical activities (Kolkowska & Dhillon, 2013:4). In most organisations, the information security policies outline the rules and boundaries that employees should adhere to. Information security policies are for employees to protect their confidentiality and the integrity of information assets (Vroom & von Solms, 2004). Further, the human factor is vital to the successful implementation of these policies. However, it is also the weakest part of the implementation of policies (Vroom & von Solms, 2004). Ensuring that compliance to policies and procedures in IT for example, has become just as important as the technical security thereof. Herath and Rao (2009a) states that technology tools are not sufficient when it comes to protecting organisational information. End user behaviour has become increasingly significant and observing this, is a challenge, especially due to research being shown, that end users have different views when it comes to security.

It is acknowledged that information security has moved away from being only technical and opened many different aspects surrounding it. This resulted in information security to take on a multidimensional character (von Solms, 2001). Today, information is the focus of most organisations where increasing legislation requirements make it complex to comply with. The IT environment organisations created do not have the benefit of having a once-a year IT audit, but created the need for a day-to day measurement and enforcement of activities (von Solms, 2006). Organisations realise the importance of complying with these regulations imposed on them (Gerber & von Solms, 2008). There is a misconception that information security management is the task of a technical nature, thus leaving security to the IT technicians. This is has been changing over recent years and is now becoming part of non-technical activities. These include the creation of policies and procedures, user awareness programs of IT risks and responsibilities, and compliance enforcement mechanisms (von Solms, 2006). According to Herath and Rao (2009a), failure in preventing security breaches in organisations are direct indicators of the lack in compliance of information security policies. The research further indicates that millions of dollars are being lost in security breaches, as a result of non-compliance or employee negligence.

According to Van Niekerk and von Solms (2010), securing information in an organisation does not necessarily generate any income and is thus often neglected. Guo (2013:244) explains that security related behaviour in organisations can be broken down into the following areas; "…computer abuses/ security contravention, unethical use, emissive security behaviour, IS misuse, violation of policy, non-malicious security violation, information security policy abuse and security policy compliance."

There are numerous threats which threatens an organisation's information security. These threats can either be, accidental, caused unintentionally by an employee, or deliberate, which is an intentional breach of security by an employee (Guo, 2013). It is a challenging task to prevent security threats from insiders within an organisation. These illegal and deviant acts are the most important threats to organisations (Cheng, Li, Li, Holm & Zhai, 2013). According to Cheng *et al.* (2013), people play a

vital role in information security governance. They could be the weakest link and therefore, the use of behavioural information security as a mechanism to combat this, is increasing. Much of the focus on information security research is on technical issues however, a significant weakness in protecting information assets, are employees in an organisation. The problem is becoming increasingly important, because researchers have estimated that almost half of the security breaches and violations, come from within organisations.

Research in the operational area of information security has been lacking until recent years according to Crossler, Johnston, Lowry, Hu, Warkentin and Baskerville (2013). Kolkowska and Dhillon (2013) state that when it comes to information security approaches, there are mainly two categories identified which are; the approaches which make use of sanctions, and the approaches which are behavioural in nature.

There have been several approaches towards holistic information security management and ultimately, these can be divided into two categories; the individual level of information security to understand why end users engage in risky behaviour, and the managerial level to understand which factors determine effective holistic information security management (Flores, Antonsen & Ekstedt, 2014:91). Literature suggests that multiple surveys conducted found that many security breaches in organisations, occur due to the actions of employees within organisations - rather than that of external hackers, many of which would not have been possible without the intentional or unintentional actions of employees (Cheng *et al*., 2013; Crossler *et al.*, 2013; Herath & Rao, 2009a). According to Flores *et al.* (2014), a significant part of research studies are towards individual information security, by testing theories with regard to compliance of information security policies. These studies inculcate the use of measures to counter security violations through training and awareness. These have proven to increase end user understanding of misuse and the consequences thereof.

### 2.2.1 Models and approaches

A deterrence model is proposed by D'Arcy, Hovav and Galletta (2009), which examines the factors relating to employee misuse intentions. The results of their

research indicate that the perceived severity of sanctions reduces information security misuse, while certainty of sanctions does not produce any significance in reducing information security misuse. Cheng *et al.* (2013:448) point out that research in this area is based mainly on the deterrence theory, and that intentions to comply can be influenced by intrinsic and extrinsic motivators. Furthermore, the research highlights that the number of studies conducted in this area does not suffice, regarding how important information security is to organisations. According to Flores *et al.* (2014) there is a significant gap in the literature that needs to be addressed in order to enhance these processes. Although there have been studies in recent years testing theories on the cause of risky employee behaviour, the findings have been inconsistent. Flores *et al.* (2014) further propose that this may be as a result of different cultural environments, thus giving evidence to the realisation that culture factors could have a significant influence on employee bahaviour.

Ifinedo (2012) proposes an integrated model, combining protection motivation theory and the theory of planned behaviour to better understand employee compliance behaviour. The findings of his research suggest that both coping appraisals and threat appraisals have a significant influence on information security policy compliance intentions.

The potential of fear as a motivator to comply with information security policies has only just started according to reported research. The possibilities for its application and many issues surrounding implementation are left unexplored. Herath and Roa (2009b) suggests that the factors influencing end user security behaviours and research in this area are still in its infancy. This is supported by Crossler *et al.* (2013:93) stating that fear motivated studies being used to increase compliance, has barely scratched the surface, leaving many issues about the topic unexplored. Fear is an underlying motivating driver contained in the protection motivation theory, and these fear-relating models are becoming increasingly important to consider, being able to increase compliance in information security (Crossler *et al.*, 2013:93).

Herath and Rao (2009a) conclude that employee security behaviour can be influenced by both, intrinsic and extrinsic factors depicted in Figure 2.1. It is reported that pressures by subjective norms and peer behaviour have a significant influence

on employee security behaviour. Further, it is reported that when complying with information security compliance, intrinsic motivation proves to be vitally important. Their research found that the severity of penalties have a negative impact on information security policy compliance. The authors finally conclude, their results path the way for future research to be conducted in this area.

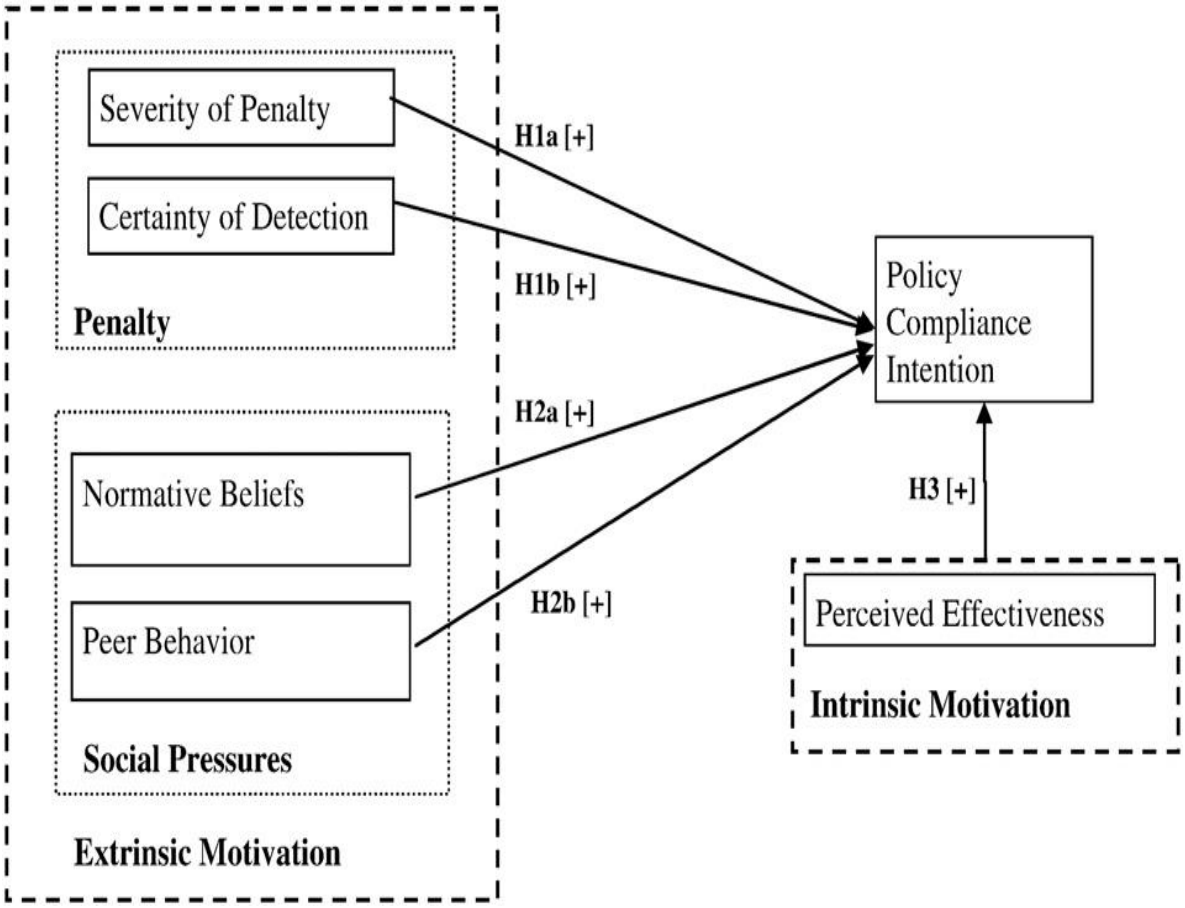


**Figure 2.1 Intrinsic and extrinsic motivators in information security behaviour (Source: Herath & Rao, 2009a:156)**

Kolkowska and Dhillon (2013) argue that the lack of compliance with policies originates from the inability to understand the intrinsic power relationships that exists in organisations. This power influences the design and implementation of information security rules and policies. Ifinedo (2012:91) investigated information security policy compliance by calling upon multiple behavioural theories. The author's results show characteristics such as "…self-efficacy, attitude towards compliance, subjective

norms, response efficacy and perceived positively influenced information security policy compliance."

Researchers over the past few years have criticised information security approaches stating that they lack theoretically grounded methods and empirical proof of their effectiveness. Thus research surrounding this have revelaed an increase in the studies to meet this criteria. This is done by introducing a variety of theories such as, the theory of planned behaviour and the protection motivation theory (Flores *et al.*, 2014).

Best practices frameworks is another approach to be considered, however, these approaches are criticised being too generic due to the fact that organisations are unique and their security needs are different (Flores *et al.*, 2014:91). Herath and Rao (2009b:154) outline that information security policies are not utilised effectively and that employees seldom comply to them. It is a challenge to enforce information security policies due to its discretionary nature, probably the reason for the recent increase in research around behavioural information security, focusing on employee intentions. Ifinedo (2012:83) suggests that the ever changing needs of organisations compels the adoption of multiple approaches, in order to be truly successful in protecting their information. Ifinedo (2014:69) further shows the effects of socialism, influence and cognition and how this influences information security policy compliance, through compliance behavioural intentions. It is concluded that the social bonds which employees share in the office with colleagues, are a major influence on the attitudes towards compliance.

According to Cheng *et al.* (2013), employee's mind-set where consequences are concerned for information security misuse, is for example, different in Korea than in the United States of America. This highlights the possibility that findings could differ from country to country, and generalising results would not be accurate. Crossler *et al.* (2013:94) suggest that behavioural information security will be extensively looked at in the future. This would provide specific research areas such as, "…specific insider deviant behaviour from insider misbehaviour, unmasking the mystery of the

hacker world, improving information security compliance and cross cultural information security research."

In light of new techniques being used to compromise information assets in organisations, the information security approaches that management will be using, is changing to adopting a more holistic approach to combat such threats. These holistic information security approaches consists on focusing more on the importance of the human element. This means that more emphasis is put on considerations such as beliefs, behaviours, attitudes, norms, culture and employee awareness (Flores *et al.*, 2014). Ifinedo (2014) states that in order to enhance knowledge, more research needs to be done around compliance from different perspectives as it is a complex topic. According to Parsons, McCormac, Butavicius, Pattinson and Jerram (2014), for training and education to be more effective in assisting information security compliance, it needs to include an understanding of why it is important. Future research needs to examine employees, organisations and factors that intervene and determine if these factors have an influence on employee behaviour, thus affecting information security compliance (Parsons *et al.*, 2014). Herath and Rao (2009b) argues that previous studies which examined security practices in organisations were often only focused on IT administrators and top level managers, thus leaving a significant gap. End users are exposed to the information in an organisation and without considering them raises the question on whether these studies are accurate in their findings.

## 2.3 Culture

In this section the researcher discusses organisation culture (Section 2.3.1), information security culture (Section 2.3.2), information security policies (Section 2.3.3). The researcher discusses these topics to provide an overview of the part the human factor plays in information security compliance.

### 2.3.1 Organisational culture

Organisational culture is a broad field that draws upon sociology, psychology and many other fields in order to understand how human beings work in groups and institutions. According to Ruighaver *et al*. (2007), security culture refers to all socio-

cultural measures that support technical security measures and that limits its focus to both sub-dimensional information and the belief that information security is a technical problem. Ideally, information security is a management problem and a security culture shows how management should deal with these problems. Consequently, it is argued that security measures and policies need to be re-designed to support an organisation's security culture. According to Veiga and Martins (2015) it is essential that the information security culture of an organisation is constantly improved in order that employee behaviour complies with information security policies and regulatory requirements.

Hinson (2003) states that there are some common human factor mistakes that take place in the workplace. There are some inevitable mistakes such entering values in the wrong fields or putting decimal point in the wrong place, or even deleting files in error. These errors are inevitable and are mostly accepted, however, employees do their best to spot and correct them before it is too late. For example, while dealing with security information, a simple configuration mistake can be made leaving a network port open, firewall vulnerability and completely unprotected systems. It is believed that human errors are likely to cause serious security breaches, rather than technical vulnerabilities (Parsons *et al.*, 2014). Scholars have gone further to argue that technical flaws in a system are products of human error thus more focus should be put on employee intentions and behaviour (Ifinedo, 2014). For example, the case of a radiotherapy machine that produces ten times the stated dose, indicates that the problem is caused by an obscure bug in the program that has escaped rigorous testing of the system. In other words, human errors are the cause of the machine's problem, but similarly, human errors could cause potential threats to information security (Hinson, 2003).

As a result of such human related problems, a new field of science; called human factor engineering has been developed, in order to resolve these kinds of issues (Hinson, 2003). For example, pressing the wrong key on a system, by human factor engineering standards, could lead to a disastrous effect, therefore, a unique key would need to be introduced to reduce such a risk. Another way of reducing such a risk would be by providing system interlocks, dual controls, as well as automatically

programmed responses. While these self-critical systems are designed, operated, tested and maintained with human safety put into consideration, the mistakes still occur. For example, power station operators sometimes press the wrong button causing accidents (Hinson, 2003).

Mitnick and Simon (2003) demonstrates how easy it is to persuade a naive helpdesk to share sensitive information with a complete stranger. The author further shows how users choose weak passwords and do not change them regularly. Mitnick and Simon (2003) also finds users share Identification Documents and misplace their smart cards thus leaving potential threats to possible intrusions. Although systems sometimes assists users to develop strong passwords, users also need to play their part to avoid human and technological problems (Hinson, 2003). Veiga and Martins (2015) propose that the human aspect be embedded into an information security culture so that instead of employees being a risk to information security they can aid in protecting information. It is often factors such as employees, policies and culture that leaves organisation vulnerable to security threats (Hu *et al.*, 2007).

According to Hu *et al.* (2007), information security systems are designed, maintained and essentially used by humans and it is therefore, important to integrate socio-economic factors when protecting such systems. To instil a culture where information is in compliance with policies and regulation is not easy and is essential for organisations to understand user perceptions, beliefs and attitudes. This will incorporate confidentially and sensitivity into a information security culture (Veiga & Martins, 2015).

### 2.3.2 Information security culture

In terms of information security itself, it is important to foster the “right” culture such that the expected aims of security are upheld. An information security-aware culture will minimise risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets. The rapid growth of information technology makes it difficult for organisations to keep up with the challenges faced in an information security culture. Cloud computing, mobile telephones and tablets are some examples of ways that employees now use and

process information, thus introducing new challenges to organisations (Veiga & Martins, 2015).

Shropshire, Warkentin and Sharma (2015) state that in recent studies personality constructs have found to show more variance in user behaviour and intentions. Herath and Rao (2009a) further discuss how to encourage information security behaviour in an organisation using penalty pressure, as well as perceived effectiveness. The authors argue that as a result of information securing becoming an important aspect of information-intensive organisation, security technologies are active been used. However, recent research has shown that information security cannot be achieved by use of technology tool alone, but can only be achieved by use of three components including people, processes, and technology (Ifinedo, 2014). On the other hand, empirical studies focusing on the effectiveness of end-user security behavior, as well as factors influencing that is still at the beginning stage (Herath & Roa, 2009a).

According to Da Veiga and Eloff ( 2010:196), "Organisations require guidance in establishing an information security-aware or implementing an acceptable information security culture.". Furthermore, PricewaterhouseCoopers (2003) find security awareness and training programmes are critical to ensure the success of information security policies.

It is the role of organisations – a subset of neoinstitutionalism (described in Section 2.6.1), to ensure adherence to appropriate protocols that adhere to external mandates for compliance. Veiga and Martins (2015) explain that an information security culture where training and awareness programmes are provided can positively influence it significantly.

Thomson and Van Niekerk (2012) discuss how an organisation can address information security apathy by employing pro-social organisational behaviour, which is seen as the fostering of positive attitudes within the organisation. The authors argue that employees are often the weakest link when protecting information assets. This is because of their apathetic behaviour whereby they lead to diffusion of

responsibility of workers. This translates to employees that believe that protecting information is not their mandate. In order to address such problems, the organisation needs to establish a culture of information security such that employee behaviours are in accordance with the goals of security information. The authors argue that there should be no communication about the thing with shared beliefs, and shared beliefs are important in the organisation because they allow the employee to interpret messages the same way.

### 2.3.3 Information Security Policies

Research by Herath and Rao (2009b) show that computer security policies are established to ensure organisational resources are protected. However, if end-users or employees do not follow policies, such initiatives started are all in vain. The author reports that efforts by organisations on social influence have a large impact on the organisational compliance intentions. Recent studies, it is suggested that there is a need for empirical studies focusing on security compliance (Herath & Roa, 2009b). On the other hand, field survey results imply that, although organisations employ technology to enhance their security measure, more effort is put on other formal, as well as informal measures such as procedures, organisational culture, and individuals addressing the security issues. Recent surveys on the main cause of security problems suggest that employee negligence is the primary cause of security problem, which has caused organisations millions of dollars (Herath & Roa, 2009b).

Veiga and Martins (2015) state that ex-and current employees in an organisation still accounts for the largest amount of security breaches. A survey by Pricewaterhouse Coopers (2014) found that ex-employees (27%) and current employees (31%) contribute to more than half of security incidents and this has risen by 25% compared to 2 years before. According to Veiga and Martins (2015) the information security culture of an organisation can significantly improve the protection of information, reduce employee risk and compliance with regulatory requirements.

Organisational security policies focus on developing process and procedures that employees follow to ensure there is the maintenance of confidentiality, integrity, as well as information (Vroom & von Solms, 2004). These security policies comprise of

company goals set by senior management, and the goals must correspond to the vision of the organisation. These policies thus provide rules and regulations that govern the security information system of the organisation (Halliday & von Solms, 1997) and also the auditing of security policies. On the other hand, research shows that scholars have paid little attention to how human factors, including individual choice and behavior or organisational factors such as culture, environment and the level of security awareness affects the attitude towards information security, as well as its management. However, such research goes further to reveal that these human and organisational factors are integral to protecting organisational assets. For this, user input is essential in addressing information system issues and strategies (Vroom & von Solms, 2004).

A weak information security culture could highten the dilemma to security breaches. For example, when employees accept as being normal to share or divulge passwords, they believe meeting customer expectations, is paramount to rather comply to policies; they may even not use any secure means of transferring information (Veiga & Martins, 2015). These potential weak points outline potential risks that could have a negative impact on any organisation as Veiga and Martins (2015) state, that information security controls has a significant impact on process, technology and information processing within an organisation. Organisations should therefore, cultivate an effective culture towards protecting information in order for it to be effective. Vroom and von Solms (2004) further argue that organisations can ensure that their employees adhere to prescribed rules and regulations by investigating the security compliance status of each individual.

### 2.4 Governance and Compliance

Information security governance is considered an essential part of corporate governance and comprises of the commitment of senior management and directors, to provide enhanced policies and guidelines (von Solms, 2001). Leaders should ensure ongoing maintenance of adequate information security measures by instituting proper organisational structures. They also need to ensure that there is an awareness and commitment towards information security. Therfore, necessary

policies, procedures, processes and technologies, and mechanisms are in place for compliance enforcement (von Solms, 2001).

Freeman (2007) reports that the fall of some of respected corporations such as, Enron, Arthur Anderson and World Con, have cost the public and the economy, billions of dollars. As a result, legislation to tighten and/or control the behaviour of corporations was introduced. These changes have led to an increased importance of the role of Chief Compliance Officers (CCO), whose function is to ensure companies comply with set rules and regulations. Although functions of CCOs become more important after the introduction of legislation to tighten the behaviour of organisations, they have been long in existance in some industries especially, those that are highly regulated. These include, financial aid and heath care to name a few. More specifically, the introduction of the Sarbanes-Oxley Act (2002) and recommendations of the United States Federal sentencing guidelines, has led to the roles of CCOs becoming more important in every organisation.

Within the realm of information security, governance refers to the leadership that can be used to implement compliance, integrate compliance with external regulations, and improve security: "…establishing information security governance is a major initiative, given the often fragmented, tactical nature of typical security efforts. It requires committed support of senior management and adequate resources. It demands the elevation of information security management to positions of authority commensurate to the required responsibilities." (IT Governance Institute, 2007:57).

According to Kolkowska & Dhillon (2013:4), compliance refers to a "…relationship in which an actor behaves in accordance with the directive supported by another actor's power, and to the orientation of the subordinated actor to the power applied…" It is noted that "…recent studies have also shown that nearly half of all companies are failing to initiate meaningful compliance efforts" (IT Governance Institute, 2007:57). Companies have introduced a program called; the Corporate Compliance Program, that assists in detecting and preventing violation of law by employees, officers and directors of organisations. The program should not be

limited only to corporations, but also to other types of businesses including partnerships, as well as non-profit organisations (IT Governance Institute, 2007).

Due diligence requires that every organisation implements compliance programs. An organisation is considered to have an effective program if it meets the following standards Firstly, the company should establish and implement a compliance and ethic program, and the board of the directors or the governing body needs to be knowledgeable about the program to offers an informed oversight. Secondly, companies need to ensure effective implementation of the program, on day-to-day basis and that the officers responsible for the program are provided with necessary resources (IT Governance Institute, 2007). Furthermore, companies should also conduct program evaluations and report the effectiveness of the program to the senior management of organisations. Thirdly, companies should avoid employing personnel who exercise substantial discretion or who have engaged in illegal activity. Fourthly, companies should have a training program whereby valuable information related to the program is disseminated to relevant people in their organisations. Fifthly, companies should also have an evaluation program to assess the effectiveness of the program, and also provide employees with the means of reporting for fear of retaliation. Sixthly, companies should motivate employees to implement the compliance program through incentives and disciplinary measures if a violation occurs. In the final place, when a criminal case is discovered appropriate action should be taken to avoid future breach of the compliance program.

A rise in the interest of information security compliance behaviour research has been witnessed, but in countries outside South Africa, creating attention to the evidence of information security violations, being different from country to country (Siponen, Mahmood & Pahnila, 2014; Cheng *et al.*, 2013; Ifinedo, 2012; Vance, Siponen & Pahnila, 2012; Herath & Roa, 2009a). Information security compliance should be seen as being completely independent from information security operational management (von Solms, 2006). External regulations are vital, but there is a cultural perception that they are unnecessary or impossible to implement.

Organisation leadership must be used to bridge the gap between information technology practices, compliance and information security. Pinder (2006) states that a way to maintaining and controlling compliance in organisations, is to have what is known as a compliance champion. This individual would identify new regulations and requirements which involve IT, be able to close the gap between legal and IT, monitor risks, ensure proper controls and budgets are implemented.

According to Pinder (2006:32), there are five questions that should be asked in organisations with regard to compliance, and are as follows:

i) Who in the organisation is responsible for maintaining an awareness of the latest regulatory and legislative requirements and how should they do this?

ii) How are regulatory and legislative requirements translated into IT terms?

iii) How can the organisation (including IT) save continually re-inventing the wheel as a result of continual compliance projects?

iv) How can added value be obtained from compliance projects that will help offset the cost of compliance?

v) How does this change the role of Information Security?

Financial institutions around the world need to have acceptable practices in order to conduct for example, legal business (Pinder, 2006). Some of these standards required by legislature include using suitable IT framework such as Control Objectives for Information and Related Technology (COBIT). Information security managers play an important role in security information and are required to be sure that there is documentation for all processes, highlighting risks and the management thereof (Gerber & von Solms, 2008). They are further required to maintain an awareness of new regulations which will affect their organisation and are required to provide a baseline for security measures and requirements. By doing this organisations can better identify gaps and introduce better controls (Pinder, 2006). The continuously improving version of the ISO standard is being adopted by many organisations as an information security management benchmark (Gerber & von Solms, 2008).

In terms of addressing information governance, COBIT divides IT into 34 processes and provides a control objective (CO) for each process (Kerr & Murthy, 2013). COBIT not only positions itself as a security tool for information technology, but it also addresses informational governance (COBIT, 2000) and other issues related to information security. To provide the way for CO to be managed, COBIT further divides the CO into a set of Detailed Control Objectives (DCOs). In the literature, studies reveal that 316 DCOs are usually developed to specify how 34 processes should be managed. The challenge is that proper IT governance will only result when each of the 34 processes is handled correctly (COBIT, 2000). The processes address different issues in IT, including security and governance. One of the processes is DS 5, which focuses on maintaining system security. Studies further show that the DS 5 process is further divided into 21 DCOs, for example, DS 5.1 and DS 5.2 which manage security measures, and identification, authentication and access respectively. Apart from the 21 DCOs, there are other DCOs amongst the total 316 DCOs that address IT security. Although other DCOs in 33 of the processes, may be approximately indirectly related to 21 of DS 5, that are also necessary for information security governance (COBIT, 2000).

The advantage of using COBIT as an information security governance framework, is that security can be integrated into larger and wider information technology frameworks provided by the other 34 processes (Kerr & Murthy, 2013). Although it is observed that COBIT is used mostly in information security governance, it can also provide the rest of the framework especially, if the company decides to base their IT governance on COBIT. When COBIT is used as the basis for IT governance, the existing IT governance fits well into the wider COBIT framework. On the other hand, the disadvantage of using COBIT as an information security governance framework, is that it does not provide enough details how to do certain activities (Kerr & Murthy, 2013).The DCOs mostly focus on what needs to be done rather that how to do it. As a result, a framework using COBIT needs to have more detailed guidelines showing precisely how activities need to be done. Bernroider and Ivanov (2011) point out that some organisations implement such frameworks without taking the time or allocate sufficient resources to investigate the appropriateness of the framework for specific tasks, also considering the specific organisational needs and culture. As a result of

COBIT being used by IT auditors for a long time, in many cases, the framework is preferred by many auditors and risk managers when conducting their jobs (von Solms, 2005).

The International Standards Organisation specification (ISO 17799) deals exclusively with information security. It is divided into ten sections which have a total of 36 objectives, which are also divided into sub-objects. The advantages of using ISO 17799 for information security, are that it provides more details than COBIT. ISO 17799 is also known to provide more guidance on how tasks need to be done. For example, ISO 17799 provides information how information security policies should be structured as well as its content. Being more detailed and technical in nature, it is in many cases used by IT managers and information security managers. On the other hand, a disadvantage of ISO 17799 is that it is stand-alone and not integrated into a wider network of information security governance (von Solms, 2005).

IT governance refers to the discharge of roles, as well as responsibilities that ensure proper IT practices are conducted in organisations. The IT governance body was established in 1998 and reports on IT governance as the responsibility of organisational senior management and directors. It is part of organisational governance with leadership and structure and processes to ensure organisational IT promotes organisational strategy, as well as many objectives (IT Governance Institute, 2006). It is however, regarded as a strategic issue that requires addressing at a strategic level.

Information security governance is a vital part of corporate governance (von Solms, 2006). Information security governance aims to protect organisation information assets and ensure the confidentiality, integrity and availability thereof. It is crucial to have an alignment between IT and business, yet it still remains a challenge (Bermejo, Tonelli, Zambalde, Santos & Zuppo, 2014).

### 2.5 Legislation and Regulations

The strongest enabler of compliance is the implementation of external regulations in the form of legislation. The context for IT and information security is such that there

are "…increasingly strident regulations and growing liabilities." According to the IT Governance Institute (2007:7), the stakes are increasing as well as hurdles being increasingly difficult to manage, especially, for small firms. The existence of external legislation creates a culture in which compliance is mandatory. Existing laws and regulations may remain vague, thus creating a context in which information security and information technology professionals must rely on law professionals, who in turn, may not know much about technology. Pinder (2006) explains that there is a gap between IT and Legal departments trying to translate laws and regulations into IT terms. and attempting to keep up to date.There is also an increasing amount of legal pressure for compliance as there has been an increase in "data-related legislation" (IT Governance Institute, 2007:58). This brings another group of stakeholders into the situation namely lawmakers. Laws can exist at many different jurisdictions and may reinforce or stand in contrast to company-mandated policies and best practices. The ultimate goal of these laws and regulations is to protect consumers and also to reduce risks (Maphakela & Pottas, 2006). The regulator as well as management need to know the cost of losses and how they can decrease these risks. An all-encompassing approach needs to be undertaken in order to mitigate risks effectively including all aspects of the organisation not excluding culture, tolerances, the control environment, operating and assurance models, details infrastructure risk assessments, risk technologies and training (Pinder, 2006).

The consequences for failing to comply with legislation can be significant for companies: in addition to or instead of merely losing customers, companies can lose its right to operate and employees can end up incaserated. Siponen *et al*. (2014) explain that employees should be trained and educated about information security policies and that managers should warn and explain the significance of these policies to employees. Organisations seeking further guidance on dealing with this may turn to the Information Technology Infrastruture Library (ITIL), which provides guidelines to organisations. There is numerous challenges organisations face in order to comply with these regulations such as additional testing required for changes and outsourced operations (Pinder, 2006).

An appropriate business system requires institutionalisation of quality internal controls and regulatory frameworks. According to Damianides (2004), the Sarbanes-Oxley Act (SOX) was enacted in 2002 to improve corporate governance, ensure organisational responsibilities, and strengthen internal controls. While SOX requires the assessment of all financial transaction of the business, the Act does not imply that the business is fully secured. For example, major banks made an effort to comply with the Basel Accord to safeguard themselves against operational, financial and technological risks. The Basel Accord is a law which aims to mitigate risks. It focuses on areas where risk must be controlled and assessed continually and include people, processes, systems, external events and other changes (Hussein & Al-Tamimi, 2008).

According to Gerber and von Solms (2008:128), the legal requirements of an organisation can be generalised into the following aspects: intellectual property rights, legislature, contractual obligations and international laws. The rapidly expanding requirements from national and international laws and regulations, force organisations to become more aware and proactive in their attempt to comply with constantly changing legal requirements (Gerber & von Solms, 2008). In most of the legislature, there are implications affecting IT departments. The implications can cost organisations up R 1, 6 billion. The Sarbanes-Oxley is one of the laws which are used to identify any system in an organisation which has an impact on financial statements. Compliance areas are large and include planning and organisation, acquisition and implementation, delivery and support and monitoring (Pinder, 2006).

According to Gerber and von Solms (2008) every organisation has a unique need for information security and this is directly related to the information security requirements it has. Once these information security requirements have been identified, steps needs to be taken to ensure risks are mitigated. These requirements are drawn from 3 sources, which include assessing the security risks, information processing of unique requirements and legal compliance.

Siponen *et al.* (2014) state that one of the most important threats to information security is from employees who do not comply with information security policies of

their organisation. Aspects such as Endpoint behaviour, attitude and personality have shown significant influence in information security compliance (Shropshire *et al*., 2015). Vance *et al.* (2012) state that more than half of security incidents in organisations are either, directly or indirectly, as a result of employees not complying with security policies.

According to Siponen *et al.* (2014) recent studies on information security policy compliance can be separated into three categories which include; conceptual principles with no underlying theory or empirical evidence, theoretical models with no empirical evidence and empirical work grounded in theory. Furthermore, they argue that the first two categories are merely guidelines and provide little insight or little evidence to support it. Vance *et al.* (2012) outline that there has been no prior research done on the influence of past and automatic behaviour on the decisions to comply by employees. Table 2.2 provides the name and brief description of the international and national laws and regulations, affecting organisations.

**Table 2.2: International and national legislation affecting the organisation**

| Law/ Regulation | Description |
|---|---|
| Financial Intelligence Centre Act (FICA) | To establish a Financial Intelligence Centre and Anti Money Laundry Council in order to fight money laundering and terrorism activities by preventing false identification (Parliament of the Republic of South Africa, 2001). |
| Electronic Communications and Transactions Act (ECT) | Used to promote the facilitation and regulation of electronic communications and transactions and to prevent misuse of systems (Parliament of the Republic of South Africa, 2002). |
| King Code | Information Security addressed as a Corporate Governance responsibility<br>Board of Directors responsible and accountable to shareholders<br>Board of Directors to ensure suitable return on investment<br>Executive management is responsible for compliance to laws and regulations and identifying and mitigating risks (Posthumus & von Solms, 2004). |
| Protection Of Personal Information Act (POPI) | Promoting minimum requirements for the processing of information. Securing the integrity of personal information in its possession or under its control by taking prescribed measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal (Parliament of the Republic of South Africa, 2013). |
| Financial Advisory | Protects the consumers of financial products and services and provides |

| | |
|---|---|
| and Intermediary Services Act (FAIS) | regulations to govern it (Financial Advisory & Intermediary Act. 2002). |
| Banks Act | Requires all banks to follow in order to provide banking services. Provides the requirements of doing business in the sector (Maphakela & Pottas, 2006). |
| Sarbanes Oxley (International) | Explicitly certifies that the organisation will accept responsibility to establish and maintain adequate financial reporting and appropriate internal control systems (Gordon *et al*., 2006). |
| Basel (International) | To improve the soundness and stability of the international banking system by promoting:<br>Minimum capital requirements<br>Supervisory review process<br>Market discipline<br>(Hussein & Al-Tamimi, 2008). |
| Graham Leach Bliley (International) | Provides a financial structure on how to protect financial information (Maphakela & Pottas, 2006). |

### 2.6 Theories, Models and Frameworks

Much of the literature on information security focusses on compliance and theories regarding how to gain compliance. The researcher specifically focussed on literature concerned with different versions of compliance theories. Most studies investigated by the researcher were on factors influencing information security compliance, mainly based under protection, rational choice and other deterrence theories (Cheng *et al*., 2013). Recent research includes various psychological factors influencing end user behaviour models such as "…moral beliefs, rational choice, self-control, accountability, disgruntlement, leadership and organisational culture." (Crossler *et al.*, 2013:92).

Compliance theories can illuminate both, organisational culture features, and notions of how compliance should work in the face of legal mandates (i.e., external necessity). Therefore, this section differs from the preceeding literature review in that it synthesises the major work on four compliance theories, and two models that lay the groundwork in an attempt to propose a conceptual framework for this research.

The following theories are discussed and expanded upon in Sections 2.6.1 through 2.6.6:

i) neo-institutional theory,
ii) agency theory,
iii) rational choice theory and
iv) the elaboration likelihood model
v) organisation culture model and
vi) a framework for the governance of information security.

### 2.6.1 Neo-institutional theory

The Neo-institutional theory has its roots in political science and sociology, although it applies to virtually any field that deals with institutions. It seeks to deal with the institution as a cohesive unit:

> "Neo-institutional theory argues that institutions are formed and changed by interactions between field and firm. It accepts that organisations and context are mutually constituent, thus actions within either analytical sphere reflexively affect both spheres. From this viewpoint, it becomes known that neither the field in which a firm operates, nor the internal workings of the firm, can be the sole source of institutionalization." (Gray, 2008:957).

Thus, neo-institutional theory focuses on context as an intertwined aspect of institutionalism.

Hu *et al.* (2007) explain that an important aspect to neo-institutional theory is that an organisation adapts to changes in its environment thus slowly becoming isomorphic with them. Hu *et al.* (2007) state that to increase the commitment from employees and external forces the organisation needs to incorporate external legitimate formal structures. The organisation needs to show that it is introducing purposes that have been collectively valued.

Neo-institutionalism is a school of thought that sought to answer specific questions regarding similarity among institutions, rather than differences:

> "The neo-institutional turn spins off from a key question that occupied the minds of researchers studying formal organisations; why do organisations

> with different goals and origins – such as large multinational companies, local research-based companies, municipalities, government agencies, schools, art museums, universities, hospitals and political parties – look so alike?" (Fredriksson, Pallas, & Wehmeier, 2013:185).

According to DiMaggio and Powell (1983), there are three isomorphic processes namely, coercive isomorphism, normative isomorphism and mimetic isomorphism. In essence, institutional theory is not normally viewed as a theory of organisational change,"… but as an explanation of the similarity ("isomorphism") and stability of organisational arrangements in a given population or field of organisations." (Greenwood & Hinings, 1996:1023). Coercive pressure is as a result of an organisation that experiences institutionalised pressure from an external organisation to which they need in order to operate, Mimetic pressure – comes about as a result of organisations needing to model themselves to copy other organisations in the environment they operate in to be successful, Normative pressure – appropriate ways to act in the organisation with regard to culture and profession (DiMaggio & Powell, 1983).

In contrast to traditional views of institutionalism, neo-institutional theory values legitimacy "…the embeddedness of organisational fields, and the centrality of classification, routines, scripts, and schema" (Greenwood & Hinings, 1996:1023). Neo-institutional theory emphasizes that the institution often may reject the legitimacy of external mandates, such as legal compliance with laws misunderstood within the institution.

Within this framework, compliance is an institutional endeavour. Since isomorphism is a defining trait of institutionalism, it would then be predictable within a neo-institutionalist framework to predict that most institutions would be relatively similar in their stumbling blocks to compliance, as well as in their methods of adherence to compliance. Neo-institutionalism essentially holds that compliance is an effort that requires the cooperation from all within the institution, even though the institution is in itself a functioning unit. An institution can decide whether or not, another institution

has legitimacy: hypothetically, a local bank has the option of deciding whether national laws have legitimacy.

According to Gladwell (2013:318), legitimacy is important for institutions, since legitimacy depends on three things.

i) People that are requested to adhere to authority need to feel as if they can speak out when the need arises and their opinion will be considered.
ii) There is an expectation that laws remain the same and not change unpredictably.
iii) The authority needs to be fair, thus there should be no discrimination of any kind.

Neo-institutionalism, in contrast to the theory discussed in the next section, would assume, for example, that management of an institution decides for itself and without individual buy-in, what is and is not legitimate (Hu *et al*., 2007).There is a strong relationship between compliance and legitimacy, because for an institution to engage in compliance, it must buy-in to the legitimacy of the thing to be complied with (Gladwell, 2013).

### 2.6.2 Agency Theory

Agency theory considers individual agency's within institutions, rather than seeing institutions as discrete agents. Agency theory essentially holds that individual or group agency spurs change, conflict and even profit within organisations. Agency theory conceptualises relationships and organisations differently from neo-institutional theory: "In an agency relationship, one party acts on behalf of another." (Shapiro, 2005:263). This means that some organisations act as agents for larger institutions, to be compliant with the law, and so forth. The agency costs can be directly related to divergent objectives that come about between agents and owners. Instead of increasing shareholder wealth, managers use organisational resources to benefit from increasing costs. Information imbalance, wherever managers discriminately have more information than shareholders, is the main reason behind these conflicts of interest. Agency prices jointly rise once shareholders try and mitigate the issues (Jurkus, Park & Woodard, 2011:180).

In essence, agency theory proposes that any institution or individual can act as an agent and does so if they act on behalf of another. Agency theory places a great deal of emphasis on discrete and defined roles within and outside of organisations: for example, within business, "Agency theory debates that shareholder interests need protection by separation of incumbency of 38 roles of board chair and CEO" (Donaldson & Davis, 1991:49). For example, agency theory has been used to assess understanding of behaviour in fields as diverse as supply chain management and business, because agency theory offers a broad conceptual framework. Agency theory has relevancy for the things whereby one party (the principal) delegates authority – in terms of management and decision-making concerning bound tasks – to a different party (the agent) (Fayezi, O'Loughlin, & Zutshi, 2012:556).

With respect to compliance, agency theory is more complicated and considers hierarchical roles and the ability of individuals to sway decision-making. Eisenhardt (1989) states that key notions of agency theory include the idea that principal-agent relationships are supposed to show the economical organisation of information and risk related costs. This further links to the agreement between the principal and the agent, determines the agency and recognizing of legitimacy, in addition to the measure to which it complies. Within this theoretical framework, communication and information are key, since information systems hampers opportunities for the agent (Eisenhardt, 1989:60), Agent theory assumes that individuals have the capacity to act and organisations consist of individuals and groups of individuals, which aggregate agency's and can make their own decisions. Any individual or group of individuals can assess legitimacy of compliance orders at any time. However, the lack of robust understanding of the nature of choice in this theory is supplanted by the next theory under discussion, rational choice theory.

### 2.6.3 Rational Choice Theory

Rational choice theory is a relatively new and somewhat controversial sociological theory as it attempts to account for the role of choice within institutions, agency and in terms of decision-making. It is based on the rationale in human actions (Zhang & Sarathy, 2009). This theory broadly assumes that "rational choice [acts] as a general

theoretical perspective, or family of theories, which explains social outcomes by constructing models of individual action and social context. “Thin” models of individual action are mute about actors’ motivations, while “thick” models specify them *ex ante*” (Hechter & Kanazawa, 1997:191). Context is important here, but not in terms of constructing the institution, as in neo-institutionalism, but instead in terms of constructing the reasons for the choices actors and agents are making. Thin rational choice models focus on trends, rather than context: Thin rational choice models have “no relationship with the specific goals that of person but is rather based on small powerful assumptions.” (Hechter & Kanazawa, 1997:194). In other words, no matter what a person’s values are it has to be stable and transitive.

In contrast, thick models are highly contextual, rather than data-driven. “Thick” models of rational choice theory, assert that “…since people have reasons for what they do, their behaviour is predictable only if we know what motivates them. Thick models therefore specify the individual’s existing values and beliefs” (Hechter & Kanazawa, 1997:194). Thin and thick models of rational choice theory correspond to some of the issues with the organisation since arguably, legal frameworks emphasize thick models that are contextual in that they rely on legal precedent, whereas information security and IT models rely on “thin” data. An appropriately integrated model must include both “thin and thick description in order to bridge the disciplinary gaps at stake in this organisation.’ (Hechter & Kanazawa, 1997:194).

### 2.6.4 Elaboration likelihood Model

The elaboration likelihood model (ELM) conceptualises and attempts to predict the likelihood that an individual may be persuaded to do something. “The ELM is based on the idea that attitudes are important because attitudes guide decisions and other behaviours. While attitudes can result from a number of things, persuasion is a primary source. The model features two routes of persuasive influence: central and peripheral.” (University of Twente, 2014). The ELM is based on seven postulates namely; seeking correctness, variations in elaboration, arguments, cues and elaboration, objective elaboration, elaboration versus cues biased elaboration, consequences of elaboration and complicating factors (Petty & Cacioppo, 1986).

Essentially, the ELM seeks to determine the likelihood of change or persuasion. It, too, has numerous applications, but within the realm of compliance and technology it can be understood to guide buy-in for new technology, decisions to comply, or even decisions to cooperate across formerly rigid institutional or disciplinary lines. "The ELM could be labelled a persuasion theory which attempts to explain and predict the effects of variables on attitudes. The basic thrust of the model is to specify the conditions under which a person is likely to elaborate on the message, that is, carefully consider the merits of arguments presented in the message. Consideration of the message depends upon which of two routes, central or peripheral, the message takes." (Gotlieb & Swan, 1990:222).

The ELM essentially "…suggests that identifying the impact of variables on the motivation to process is necessary, but not sufficient for predicting the effects of arguments presented in a message. Managers and researchers must identify both motivation and ability to process the message to predict the effects of a message on attitudes." (Gotlieb & Swan, 1990:221). Therefore, the ELM is useful within the field of compliance because it helps to predict and assess potential outcomes. It unifies tenets of agency theory, along with aspects of the other theories mentioned above.

### 2.7 Organisational culture model

Organisational culture is a complex phenomenon with many debates surrounding the area on whether it can be measured or not (Hu *et al.*, 2007). The consensus of the topic is limited because of the unique nature of it (Veiga & Martins, 2015). The culture of an organisation is different from company to company and for it to be predicted, is seen as a challenge in the research community (Denison *et al.*, 2004).

Denison *et al.* (2004) propose a framework for organisational culture by using data collected from more than 764 organisations. The framework of the authors concludes that there are 4 cultural traits which is seen in every organisation and had proven to be effective. These traits are; mission, adaptability, involvement and consistency. Mission and consistency prove to be a good predictor of profitability and involvement and adaptability proves to be a good predictor in the growth of sales. According to

Denison *et al.* (2004:100). These dimensions can then be further categorised into sub-dimensions as follows:

**i) Mission - strategic direction and intent, goals and objectives and vision**

A successful organisation has a clear and concise vision, mission, goals and objectives and is communicated to employees regularly. Employees align these principles to their work to better achieve the organisations purpose. Effective organisations find the balance between the top down and bottom up approaches both having their own challenges in implementing direction and focus (Denison *et al*., 2004).

**ii) Adaptability - Creating Change, Customer Focus and Organisational Learning**

An organisation which adapts to its constantly changing environment is one which will be successful. An organisation which is well integrated does not necessarily mean it will easily adapt to change. An organisation which uses their customers' needs to drive change in the organisation is able to keep up with the forever growing competitive environment in which they operate. They should always be improving, taking risks and learning from their mistakes in order to give better value to their customers (Denison *et al.*, 2004).

**iii) Involvement - empowerment, team orientation and capability development**

Organisations that empower, grow and develop their employees are found to be much more effective than those who do not. By investing in their employees organisations benefit from more committed, capable and involved employees. Employees align their goals to the goals of the organisation and this directly increases the value of the employee to the organisation and the organisation to the employee (Denison *et al.*, 2004). Figure 2.2 depicts the cultural model as proposed by Denison *et al.* (2004).

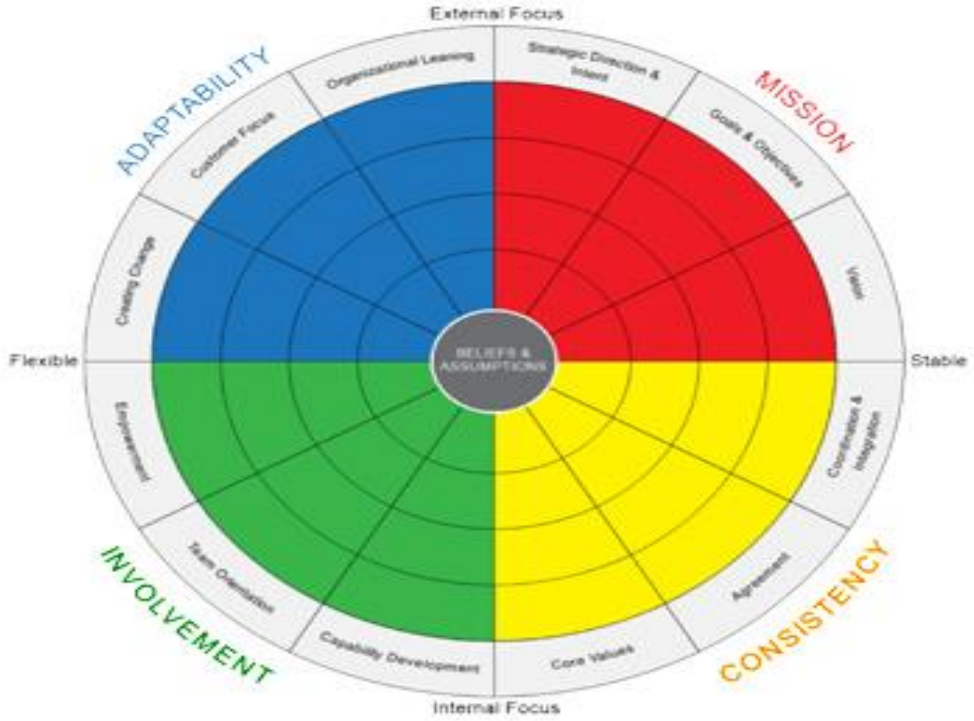


**Figure 2.2: Daniel Denison's organisational culture model (Source: Denison *et al*., 2004:101)**

### iv) Consistency - Core Values, Agreement, Coordination/Integration

It has also been found that organisations are more effective when being consistent, well-coordinated and well integrated. Employee behavior stemms from a set of values from which the organisation is operated from and called upon by management decisions**.** This results in a strong sense of consistency and stability amongst employees that is around this constant mindset (Denison et al., 2004).

## 2.8 A Governance Framework for Information Security

Information security is perceived as maintaining of confidentiality, integrity and availability of information. This is done through various control mechanisms through physical, technical and operations security. This could include characteristics such as, access control, password control, information security policies and network security. Information security has a major influence of the trustworthiness of an organisation and ultimately affect relationships with internal and external stakeholders involved with the organisation (Posthumus & von Solms, 2004).

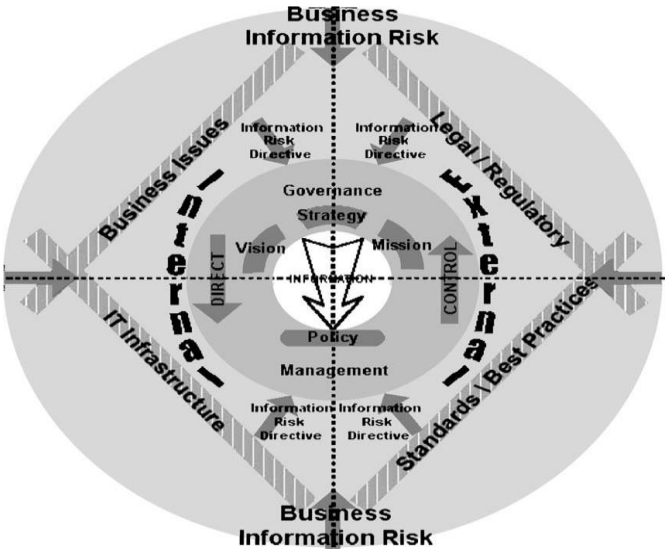


**Figure 2.3: A Governance Framework for Information Security (Source: Posthumus & von Solms, 2004:645)**

External risks have the potential to effect organisations from the outside. These can be natural or technical risks. Natural risks could be natural disasters, flooding, fire, earthquakes, and lightning. These natural disasters have the potential of incurring devastating effects on organisations and its infrastructures. Technical risks are those that arise from technology including the storing, processing and dissemination of information within organisations. These risks can arise in hardware or software failures and may cause significant potential losses for organisations. Finally, there could possibly be deliberate attacks from hackers that could be trying to damage or appropriate information from organisations (Posthumus & von Solms, 2004).

Internal risks arise from within organisations and have the potential to effect organisations from inside. These include potential human related risks which pose the greatest potential threat to organisations. Human related risks could be deliberate such as, viruses through flash drives and email attachments, or by deliberately exposing an organisations network for malicious attacks and hackers. All internal risks are not deliberate and we see cases of employees merely making mistakes such as deleting sensitive information, not securing their logins, or capturing wrong information. This is a major challenge for organisations to deal with and proper attention should be given to these potential risks when addressing these risks (Posthumus & von Solms, 2004).

The management of an organisation is tasked to implement and enforce instructions from the Board of Directors (BOD). They are responsible for maintaining and reporting everything to the executives for decision making. Management has an essential role to play as they will be the implementers of tinformation security controls and policies (Posthumus & von Solms, 2004).

The BOD is responsible for directing and controlling organisations. They are needed to oversee the best interests of the organisation. Information security is one aspect that needs to be implemented from a top-down approach and starts at director level. The King Code stipulates that the BOD is ultimately responsible for organisational decisions and be fully committed to implementing the organisations vision, mission, strategy and policies. This is done through regularly reporting from management and BOD meetings (Posthumus & von Solms, 2004).

The need for regulation has become increasingly important with the rise in the ease of access to the information of organisations. The open and accessible networks which were stimulated for adoption and growth, can become the very threats to an organisation (Posthumus & von Solms, 2004). Regulations and legislature are crucial elements that are used to protect customers and organisations across the world. Examples of these in South Africa are, the Financial Services Board, Financial Intelligence Centre Act, Electronic Communications and Transactions Act and the Protection of Personal Information Act.

Business issues relates to the need of an organisation to have their information secured. Organisation require their data to have integrity, to be available and to be confidential at all times. An organisation's information is its most important asset and needs to implement security controls in order to protect it. These security controls should align with the values and goals of the organisation in order to sustain it (Posthumus & von Solms, 2004).

IT infrastructure is commonly referred to as the backbone of organisations. The need to protect it physically and technically, is of high importance. The IT infrastructure

stores, processes and communicates all the information of the organisation and poses a great threat in terms of potential risk to the organisation. In order to mitigate these risks risk analysis and management needs to be done regularly (Posthumus & von Solms, 2004).

Information security standards and guidelines provide a means to build trust between organisations and their stakeholders. By using information security standards and guidelines, they contribute to global standards and best practices within the industry in which they operate. These standards and guidelines are highly important and assist organisations to manage their organisations more effectively and efficiently while enabling them to protect their information (Gerber & von Solms, 2008).

## 2.9 Summary of compliance theories

In Table 2.3, the theories reviewed in this chapter are summarised. Links to these theories are made in order to illustrate how the theories relate to information security and compliance.

**Table 2.3: Summary of the compliance theories and models (as discussed in Chapter 2).**

| Theory/ Framework | Construct | Variable |
|---|---|---|
| Neo- Institutional Theory | Coercive isomorphism | Regulatory pressure |
| | Normative isomorphism | Client and Stakeholder pressure |
| | Mimetic isomorphism | Industry pressure |
| A framework for the governance of information security by von Solms (2004) | Governance | External risks |
| | | Internal risks |
| | | Strategy |
| | | Vision |
| | | Mission |
| | | Policy |
| | | Management |
| | | Legal/Legislature |
| | | Business issues |
| | | Standards |
| Daniel Denison's (1990) organisational culture model (Denison *et al*., 2004). | Culture | Mission – Strategic Direction and Intent, Goals and Objectives and Vision |
| | | Adaptability – |

| | | |
|---|---|---|
| | | Creating Change, Customer Focus and Organisational Learning |
| | | Involvement - Empowerment, Team Orientation and Capability Development |
| | | Consistency – Core Values, Agreement, Coordination/Integration |
| Agency Theory | Principal/ Agent | Establishing Legitimacy |
| Rational choice theory | Rationalization | Employee view in benefit with complying |

## 2.10 Proposed Conceptual Framework

Using the literature review, a conceptual framework should be developed that could include aspects of each theory described in Table 2.3. For the purposes of this research, a conceptual framework is proposed in Figure 2.4, that synthesises each of the theories discussed. For this research, a neo-institutionalist framework's understanding of context and of institutions is combined with the agency theory. This is needed because agency theory is believed to be more important in terms of addressing the institutional and disciplinary boundaries that exist within this organisation. Agency is inscribed at the departmental and job level and ELM is called upon in order to predict buy-in and the willingness to communicate across disciplinary boundaries. That is, the study assumes that individuals who work at the organisation are capable of making decisions and further, that the notion of "information security" individuals and "legal compliance" individuals is itself tied to concepts of both agency and of neo-institutionalism. The framework then incorporates the aspects for the governance of information security by von Solms (2004) such as external and internal risks, strategy, vision, mission, policy, management as well as legal and business issues. Thereafter, the researcher integrated it with Denison's organisational culture model (Denison *et al*., 2004). The influence in which the culture of the organisation affects the organisation's information security compliance by means of cultivating the mission, adaptability, involvement and consistency dimensions. The decisions and communicative choices

each individual makes, are part of a complex matrix of factors and contexts. However, the stakes here are simply to remedy the strict boundaries within organisational culture and to ensure a culture of compliance with external legal regulations. This is done by creating internal regulations and protocols that strengthen market position by mandating the highest standards for information security within the organisation.

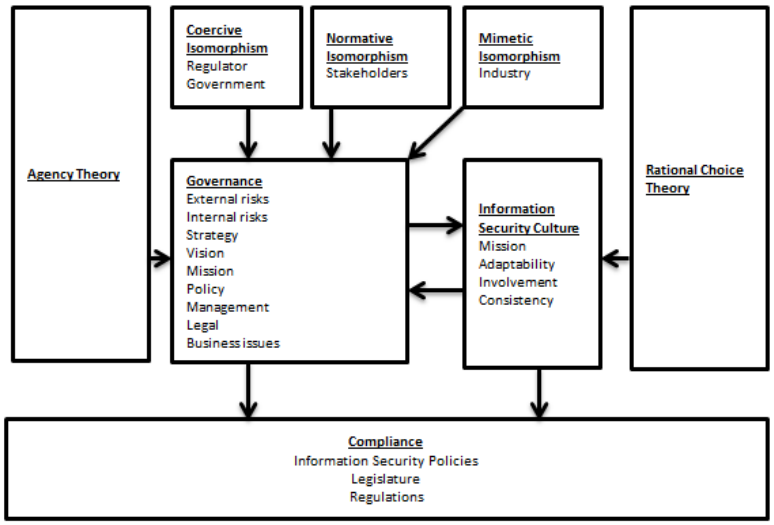


**Figure 2.4: Proposed conceptual framework**

## 2.11 Summary

The literature clearly points to the increasing rise in interest in information security compliance behaviour. Organisations handles huge amounts of sensitive information and to protect this information is essential, even critical. Many laws, regulations and policies have been put into place as a result, however compliance still remains a growing concern. By including the human factor in these rules and procedures this could potentially assist in compliance objectives.

The factors consisting of both, the strengths and weakness, which influences information security compliance, plays a vital role and by understanding this, and exactly in which way this is done, results in a framework as shown in Figure 2.4. This would assist organisations to reach their compliance objectives by including human factor and theories that apply to a specific organisation.

The following chapter covers the research methods and design to conduct the research for this study. Chapter 3 includes the research philosophy, approach and strategy. This is followed by data collection, analysis techniques and ethics.

# 3. Research Methodology

## 3.1 Introduction

In this chapter the researcher outlines the research design process, research philosophy, research approach, research strategy, data collection, and data analysis techiniques in Sections 3.2 through 3.7, in order to fulfil the requirements of this research. The researcher also discusses the ethical considerations taken in order to conduct this research, given in Section 3.8. The research aim, proposed in Chapter 1, Section 1.3, which this thesis adheres to, is that fragmented information security compliance approaches and implementation, creates uncertainty and failure of quality compliance within organisations. As a result, this may lead to reputational damage to the organisation. It is evident in Chapter 2, Section 2.3, that culture in an organisation plays an influential part in information security compliance. From the literature, it is found with the rise of threats to information security compliance, new approaches are needed in order to achieve an organisations information security compliance goals. The research design includes all the relevant factors found in Chapter 2 that influences information security compliance.

## 3.2 Research design process

Research methodology is referred to as a science, investigating how research is to be conducted. It describes the procedures which researchers need to use to carry out tasks, the research process giving descriptions, explanations and predict several phenomena (Myers, 2010:357). Research methodology provides researchers with a work plan. It is important for a researcher to select appropriate methodologies for the chosen problem. Within the research methodology, the researcher needs to have an understanding of the research process. One benefit of research methodology is that it ensures that the researcher is involved and is constantly active in the research process (Bryman & Bell, 2011). In general, the research methodology maps out the entire process and ensures that it maintains credibility (Baxter & Jack, 2008). The correct and applicable research methodology is influential to the entire research process.

The aim of the research as mentioned before, is to explore how fragmented compliance approaches affect employees to comply with laws, regulations and security policies regarding information in an organisation. This will be done in order to confirm whether governance and human factors play any significant part in compliance. The research is exploratory and specifically analysis the governance function of stakeholders who influence its information compliance operations. The researcher asks questions whether organisational culture and the human factor, actually influence employee's compliance to laws and regulations. This is done in an attempt to determine which factors ultimately have the most influence, and exactly in which way these factors influence employee's compliance to laws and regulations. The findings will add to the body of knowledge and assist future researchers in the quest to acquire knowledge. The researcher maintains a holistic approach to information security compliance by combining different approaches and facets on the topic. The research is based on aspects using Neo-institutional theory, agency theory, rational choice theory and a framework for the governance of information security, proposed by von Solms (2004) and earlier work by Denison (1990), on an organisational culture model.

> The research problem that the thesis aims to answer is that; **Fragmented information security compliance approaches and implementations create uncertainty and failure of quality compliance within organisations, with the result that it may lead to reputational damage of the organisation.**
>
> The research questions are**: i) What factors do organisations face in order to comply with laws, regulations and information security policies? and ii) How does the information security culture influence compliance to information security policies and regulations?**

In order for the research to be conducted in an organised manner, a seven-step process proposed by Warden (2007:30), would be adopted, and carried out as follows:

Preliminary literature review, identifying the research problem, formulating the research question and sub-questions, in-depth literature review to support research

question and sub-questions, collecting evidence from respondents, analysis of findings and results, conclusion and recommendations.

### 3.3 Research philosophy

Research philosophy is built on two main pillars, namely, the ontology and epistemology approaches. In the next section, these two approaches are discussed.

#### 3.3.1 Ontology

Ontology is seen as the nature of reality, which may be based on either, subjectivism or objectivism (Saunders *et al.,* 2009). The central question which gives the entire ontology, its perception is whether the existent social entities need an objective or subjective perception. These (objectivism and subjectivism) constitute the two most important aspects of ontology. According to Saunders *et al.* (2009:110) subjectivism is about "…social phenomena which is created from the perceptions and consequent actions of those social actors concerned with their existence." On the other hand, objectivism is when the existence of social entities in reality is independent and external to the social factors which result in such existence (Saunders *et al.*, 2009). The argument used in objectivism is the question of how or whether to establish and give proof that some specific action is either right or wrong. Objectivism can also be referred to as epistemological realism. This is a theory which gives the indication that the existence of reality is independent of the mind (Bryman & Bell, 2011).

The first type of ontology is descriptive ontology. This refers to the collection of information which is prima facie. Such information may be within some specific analysis domain or may be in general (Saunders *et al.*, 2009). The next type of ontology is the formal ontology. Formal ontology carries out the distillation, filtration and codification of results. Formal ontology is formal in the sense of logical investigations. With this, formal ontology mainly deals with processes, things, parts and whole, matter plus numbers. These can be said to be pure categories which characterises aspects of reality, or types of reality. However, they still have little to do with the applications of any formal realism. Formal ontology can be differentiated from formalised or codified ontology by referring to it as categorical ontology (Brannick & Coghlan, 2007). Formalised ontology mainly exists within the third step of construction of theory. At this level, one is charged with the task of finding the

appropriate formal codification. Formal codification, is the next type of ontology and its constructions relate to the adequacy for the various forms of formalism.

In the field of IT, ontology can be termed as the working model which gives a representation of the interactions of entities in some specific knowledge domains and knowledge practices, plus the entities themselves (Brannick & Coghlan, 2007). An example of such a field of knowledge is electronic commerce. Ontology gives a specification of the conceptualisation which humans and programs make use of while sharing knowledge.

The importance to determine ontology during the initial stages of the research is that it defines the choice of research design. Identification of ontology results in a choice of the approaches and methodologies used in the research process (Bryman & Bell, 2011). Examples of the methods include: experimentation (deduction) and case studies (induction). The research strategy employed in this research is the use of a case study. The ontology for this research is based on subjectivism. Selecting subjectivism also referred to as constructivism, which leads to a choice on interpretivism epistemology. Aligning the research to the inductive approach chosen for the research to collect and analyze the data, the research incorporates qualitative methods when collecting and analyzing data.

Subjectivism is used in this research in order to bring out the best answers of participant experiences and interpretations. The research was conducted in a value-laden manner, stressing the relationship between the researcher, subject and constraints. Subjectivism implies that knowledge is only created through observation (Bryman & Bell, 2011). In this case, the research seeks to establish the relationship between the legal departments and the information security departments. The research is aimed at identifying an improved means to implementing a successful information security compliance method. A subjectivist ontological stance was followed.

### 3.3.2 Epistemology

According to Neuman (2010), epistemology refers to the nature of knowledge and what constitutes acceptable knowledge, which is one of the basic questions of epistemology. Epistemology gives a description how humans think. It attempts to

differentiate right from wrong. There are instances when epistemology is termed as knowledge theory. Epistemology can be seen as the relationship between the knower and the known, while one gets to know reality and discover truth in a subjective or objective manner (Saunders *et al.*, 2009). The authors view epistemology when knowledge is acceptable in a field of study. This research takes a subjectivist ontological approach and is approaching the research from an interpretivistic way of thinking, because the research is conducted amongst people rather than objects (Bryman & Bell, 2011).

Epistemology is defined as the validity of the senses of humans and highlights them as the main way to gain information and knowledge about the world (BonJour, 2010). Epistemology entails viewing reason as the means to gaining or acquiring knowledge plus understanding. On the other hand, logic as per epistemology refers to the means of maintaining the set of knowledge (BonJour, 2010). However, there is the need to associate the knowledge gained with reality. This is done through using objectivity. Objectivity can be a measure of the validity of knowledge. Additionally, epistemology also involves the view of the concept and refers to it as abstracts giving specific details regarding reality or any other forms of abstractions. There is a need for a proper or rational epistemology when it comes to conducting a research.

There are two major approaches to epistemology. The first is rationalism and the second is empiricism. According to rationalism theory, knowledge is gained through reasoning (BonJour, 2010). The second approach (empiricism) holds a contradictory view that knowledge is gained through making use of sensory experiences. However, most of researches indicate that both epistemology approaches are needed for one to gain knowledge. Rationalism epistemology focuses on what can be termed as a necessary truth, an example being self-evident truth. On the other hand, empiricism has its focus on synthetic truth. This type of truth has its source in the sensory experiences which one has of the world (Zagzebski, 2009). The research used an interpretivisist approach. Interpretivism describes researchers aiming to get a better understanding to the issues in question.

According to Brannick and Coghlan (2007:63), epistemology is "…the study of justified beliefs and knowledge". There are specific aspects of knowledge which is concerned with epistemology. The first, are the necessary and sufficient knowledge

conditions. The second, are the sources of such knowledge. The third, are knowledge structures and the limits placed on all the forms of knowledge. Epistemology, being a study of justified beliefs seeks to establish whether justification is internal or external to the minds of humans. This research follows an interpretivist philosophy.

### 3.4 Research Approach

Research approach refers to the plans and procedures that are followed to conduct the research (Baxter & Jacks, 2008). Research approach entails the steps from the broad topical assumptions within a research to the points of collecting, analysing and interpreting data. The first two main approaches are quantitative and qualitative (Bryman & Bell, 2011). Quantitative approach has its links with the positivist paradigm where data is collected and analysed in numerical form. The analysis results in statistical calculations which are used to draw conclusions (Baxter & Jacks, 2008). In a quantitative approach, there is the development of several hypotheses. The use of statistical analysis extends a great way, allowing researchers to discover several complex and causal relationships between variables, and how changes in one variable influence others. A qualitative approach has its associations, mostly within the social constructivist paradigm. This places its emphasis on reality which is socially constructed.

The approach to theory development is one of induction. Within inductive approaches, a researcher is expected to start the process from data collected, the researcher then needs to take an overall view of the data (Bryman & Bell, 2011). The steps of an inductive research approach starts with observations made by the researcher, and proceeds to the theories which are later formulated when approaching the end of the research. The researcher seeks to find patterns within the data and normally develops a theory. An inductive approaches begins from observations and moves to more general proposition sets (Baxter & Jacks, 2008). In contrast, a deductive approach is the reverse of the inductive approach. Instead, researchers start the process by first identifying a social theory of interest, and then carries out research to establish how such theories implicate observed data. Further, a deductive approach moves from a general level of data and information which is then narrowed down, to a level which is more specific. This research is in the field of

information technology, which is a science. A deductive approach is thus mostly associated with scientific investigations (Saunders *et al.*, 2016).

Descriptive and empirical approaches are also other approaches to qualitative research. A descriptive approach entails surveys to be conducted by the researcher in order to find facts of different kinds (Baxter & Jacks, 2008). Descriptive research intends to give a description of the state of affairs, in the manner they exist currently. A researcher selecting a descriptive approach has minimal or no influence over the data variables and is only in a position to provide a report on the status of the phenomenon. Furthermore, under a descriptive approach, all the methods of research used in the collection and analysis of data are survey methods. This also includes comparative and correlation methods. One downside to this approach is that the researcher is obliged to use data which is already available in order to carry out the analysis to reach a critical evaluation of the material or phenomenon under investigation (Baxter & Jacks, 2008).

Empirical approaches place most of their reliance on the experiences and observations only. There is little importance placed on systems and theories when a researcher takes up the empirical approach. An empirical approach is data based research which focusses on providing data and information capable of any form of verification with experimentations and observation. It can also be referred to as experimental research. The initial steps of research approaches comprise of fact finding. Such data are then simulated in order to gain the required information for analysis. One of the characteristics of an empirical approach is that there is a possibility of the researcher to manipulate one or more of the variables to see the effects of the results it prosempirical research approaches (Baxter & Jacks, 2008).

The main reason for selecting an empirical approach is to gain proof that certain results within a phenomenon are caused by changes or alterations, within specific variables (Bryman & Bell, 2011). This research is a descriptive study with an inductive approach. The inductive approach involves developing a theory and testing it. Qualitative methods are used to collect data. The qualitative approach is the primary method for data collection and analysis.

### 3.5 Research Strategy

This research is a case study of an asset management organisation. Yin (2003:15) defines a case study as "…an empirical inquiry within its real-life context, especially when limits between the phenomenon and setting are not clearly observed". A case study is defined as "…an investigation of a real world scenario within a given context." (Saunders *et al.*, 2009). According to Fisher, Buglear, Lowry, Mutch and Tansley (2010), a case study enables researchers to give a holistic account of subjects under investigation. It helps to focus on the interrelationships between all the factors such as people, groups, policies, and technology that make up the case study.

Case study research is effective to assist to understand complex phenomenon and it also adds value to previous research on a similar matter. Case studies tend to be more focussed on empirical enquiries on contemporary phenomenon (Gerring, 2006). The setting of such phenomenon is on their real-life context. Initially, the preparation and determination of the research questions needs to be finalised (Yin, 2013). These questions are determined during the first stages of the case study research. The research might be carried out on complex phenomenon. The research questions provide focus for the research and are a point of reference during the process. A wide range of questions on the research unfolds due to the fact that each of the objects has a connection with the social, political, personal or historical issues. In depth investigation of the phenomenon is carried out as the researcher attempts to find data or information which answers the research questions (Gerring, 2006).

Secondly, in case study research the researcher needs to select various cases and also choose which techniques to use for gathering and analysing data (Yin, 2013). These techniques are chosen based on whether the research is set to investigate single or multiple cases. Referring back to the purpose of the research in Section 3.2, is one way to ensure the techniques selected are appropriate.

Thirdly, the preparation and collection of field data is considered (Gerring, 2006). Data collected is from multiple sources. Here the researcher collects data from various personnel, within different levels of the organisation. There is a high level of

importance placed on the researcher's attempt to constantly maintain a relationship between the data or information collected, and the research problem.

The final step is the analysis of data. The researcher carries out an analysis of the raw data and considers several interpretations in order to find linkages which may exist between the research problem and the research questions.

With case studies, researchers carry out in depth studies of some specific situation or scenario, instead of just conducting a general statistical sweep or survey (Baxter & Jack, 2008). The researcher uses a case study to narrow down the research area, which in this case is IT. The advantage of gaining focus the researcher followed the research process using the case study approach. Qualitative case studies allows for the analysis of the phenomenon through using different data sources (Yin, 2013). Additionally, the use of a case study in the research enabled the researcher to determine and investigate the implementation and use of scientific models and theories in the real world.

Analysis of data collected from the case study are opinion based, giving a representation of the opinion of the researcher and the respondents of interviews. Ontology and epistemology are both concerned with the societal contexts of right and wrong. On the contrary, a case study does not consider this. Case studies are more of opinionated (Yin, 2013). Data is collated in a manageable form and a narrative constructed around such data to give explanation and conclusions. Data collected from the case study, using the interviews and the subjectivist ontological approach, is used in order to ensure the information from the research validity.

### 3.5.1 Unit of analysis

The unit of analysis is the phenomenon which takes place within a bounded context. The case forms a basis for the research. The unit of analysis is determined through different sets of questions. Examples are; do I want to analyse the difference or similarities between organisations? Do I want to analyse a process? Do I want to analyse a program or an individual? These give a definition to the scope of the research size (Brannick & Coghlan, 2007). Developing the unit of analysis is also important for eliminating the broadness of the research. It narrows down the topic to be researched on, resulting in more specific data and information.

This research focusses on operations carried out by the legal departments and IT departments, in attempting to protect the customer assets for the financial services firm. The units of analysis are the employees who deal directly with sensitive information in the organisation. They include the head of departments, IT department, financial advisors, accountants, investment analysts and the legal department of the organisation. There are 21 participants interviewed ranging from senior, middle and low-level employees. The sample was selected using non-probability sampling. The researcher adopted purposive sampling which allowed the researcher to be able to source better candidates to answer the research questions.

### 3.6 Data collection

Generally, there are three ways in which a researcher can collect data while carrying out qualitative research, namely, observation, interviews and questionnaires (Wilson, 2014). These methods can be carried out in a variety of ways. Conducting semi-structured interviews is a method for collecting qualitative data for research puposes. According to Wilson (2014), semi-structured interviews are seen as a hybrid of structured and unstructured approaches, based on structured questions, but also allows for greater flexibilty for interviewer and interviewee. Semi-structured interviews are best to use when there is only one chance of interviewing respondents, such as is the case with this research (Whiting, 2008). The benefit of using semi-structured interviews is that despite the guide and questions being prepared early on, there is a chance for informants to give their own views regarding the research subject matter.

In semi-structured interviews, the respondents, plus the interviewer are involved in a formal interview. The onus is on the interviewer to develop an interview guide and to make use of it. The interviewer uses a list of questions related to the research and sub research questions using an interview guide (Whiting, 2008). These are to be covered in a particular order, set by the interviewer during the interview. The interview is semi-structured even though the interviewer makes use of the interview guide. Guidelines within semi-structured interviews aim at providing comparable and reliable qualitative data.

The data in this research is collected according to an interview guide (Appendix 1), using semi-structured questionnaires. Interviews takes place at senior, middle and lower levels within the organisation, in order to determine the extent of compliance practices and obligations. The participants are chosen purposively in order to target people who would best answer the questions. The questions contained within the interviews are open-ended in order to allow the respondents to give their views on the subject matter. Additionally, the interviews are all tape-recorded and later subjected to transcription and validation for further analysis.

### 3.7 Data Analysis

According to Wilson (2014), analysing qualitative data can be very time consuming and often deals with large amounts of data. The author proposes four analytical steps to analyse data from interviews, which can be summarised as; transcribing the data, reading and generating categories, creating themes and patterns, interpreting the findings and writing a report. These steps are followed when the research data is analysed:

i) The first step is transcribing data ready for data analysis. The researcher transcribes data by transforming that which was collected from the interviews in terms of spoken words, and changing this into a written form in preparation for analysis (Appendix 2). The justness of the transcription is a major factor to bear in mind to maintain the accuracy of data collected. There are both, opportunities and challenges, which are associated with interview data transcription. Transcription challenges, mostly appear from hastiness of researchers to conduct data analysis. With such haste, there is a chance that researchers may choose a transcription technique which is not fully appropriate to achieve the objectives of the research (Wilson, 2014).

   Transcription is normally an act conducted behind the scenes. However, it is crucial in the representation of correct information gained from interview records. There are multiple ways to conduct transcription. Firstly, it can be through the use of naturalism. With this technique, every single utterance form interviewee respondents is

captured to the deepest depths possible. Another means is through de-naturalism. Naturalism and de-naturalism within the context transcribing interview data, and are mainly a means of representing the interview language. Here, grammar and other influences (noises) from the interviews are corrected to enhance the validity of the data acquired. Transcription decisions available to researchers, the impact that such decisions may have on the research process, and the results are all contributing matters to incorporate when reflecting on the entire process (Wilson, 2014). Transcribed interviews are given to the interviewees to validate afterwards, to ensure the transcriptions are a correct version of the truth.

Ii) The second step is to read and generate categories, themes or patterns. This is the main analysis stage of the research data. At this stage, the researcher reads through all the collected data. The comments gained from the respondents are then organised into similar categories using a coding technique. The categories are organised in terms of the strengths, weaknesses, input and output recommendations, amongst others. Additionally, the categories or themes are further labelled to avoid any form of confusion. Patterns are also detected within the data. The researcher considers patterns such as, the number of respondents who agree that the organisation is compliant to the legal requirements. The commentaries at this analysis stage are kept for future references.

ii) The third step is to interpret the findings of the research process using the themes or categories discussed above. Interpretation is the process which aims to put the information gained from the data into perspective to the research problem and research questions under consideration (Ford & Wiedemann, 2010). During interpretation, the researcher carries out a comparison between the expected results and the actual results. There is the probability that to some extent, the organisation is compliant to the legal requirements and both, the information technology and legal departments carry out practices to

ensure this. The interpretation of the findings seeks to establish the extent to which such compliance exists in the organisation. The variances prompted the formation of recommendations which aims to rectify such recommendations is made after the conclusions to the processes is reached.

iii) Finally, the writing of a report after data analysis is completed. The scope and level of the report content is determined by the personnel to whom the report is intended. The report represents the information collected from employees (Gerring, 2006). Therefore, it is appropriate that the employees are in a position to read and interpret the report in relation to their work areas and job level. The report contains the details about the whole research project. The report also contains the research plans and activities. Additionally, the report provides a record from which future references can be made for whatever reason.

### 3.8 Ethics

According to David and Resnik (2011:1), the definition of ethics is the "…norms for conduct that distinguish between acceptable and unacceptable behaviour". There are many different reasons why ethics is so important in conducting research. The most important of them would be to promote the goals of research in general by searching for the truth, to promote the values that are essential to work together by being trustworthy, and to ensure that the researcher can be held accountable for his research (David & Resnik, 2011).

The researcher will be honest in all communication with the organisation and in the representation of data collected (Appendix 3). The researcher will strive to be unbiased in my data analysis and in all other aspects where this will be required. The researcher will be careful in order to avoid errors and negligence in my research. The researcher will maintain being sincere in my methods of obtaining data by always trying to keep my word. The researcher will share all results with the organisation if they choose to ask for them and ensure all my research remains transparent. The researcher will endeavour to uphold honour and be aware of the

implications of intellectual property and give credit to any contributions made to this research, and not use any data without permission. Voluntary consent has been given from the organisation and participants (Appendix 3). The data gathered will not be used to damage the reputation of the organisation. The name of the organisation will remain anonymous throughout the research to maintain confidentiality of the use of the information. The researcher will respect all participants in the research process and everyone will have a choice of whether or not, they wish to participate. Participants are able to refrain from participation at any time during the research process. Discrimination is avoided at all times participating in the research. Informed consent has been received from all participants and they have the right to stop participating in this research at any time they feel compelled to do so. The researcher will endeavour to prevent any harm occurring to the research participants and to the organisation. The research will aim to strengthen the organisation by equipping it with useful information to formulate strategies in the future to counter non-compliance. The researcher will at all times endeavour to avoid any act that would harm the research participants and organisation's trust and always treat all information as confidential. Research will be conducted during less disruptive times at organisations not to disturb working hours of participants and organisations. All findings will be revealed to organisations if requested and used in whatever manner they see fit.

### 3.9 Summary

The thesis proposes an integrated framework by including the human factor when complying with information security compliance objectives. The research will determine the factors which organisations face in order to comply with laws, regulations and information security policies as well as the way information security culture influence compliance to information security policies and regulations. The research uses a qualitative approach by means of a case study that was used to evaluate whether this approach provides a superior means of resolving the legal-technological gap. An interpretivist stance from a subjectivist ontology guides the research. The research approach was inductive and a case study was used as a research strategy. Data is collected by means of 21 interviewees using an interview guide, to assist and guide the interviewer throughout the interview process. The

interview guide consists of semi-structured questions. Data is analysed by means of summarising, categorising and thematic analysis.The ethics and research process is approved by the CPUT ethics committee and CPUT research proposal committee.

The following chapter (4) represents the findings of the research. Chapter 4 includes the introduction, the case, the findings, and summary of the findings.

# 4. Findings

## 4.1 Introduction

In this chapter an introduction to the aims of this research is revisited, followed by a description of the case study used in Section 4.2, followed by the discussion of the findings in Section 4.3. Finally, the chapter ends with a summary of the findings and links the research questions with the theories and themes, developed in Section 4.4.

Fragmented compliance approaches and implementations create uncertainty and failure of quality compliance within organisations, and as a result, may lead to reputational damage to an organisation. The aim of the research is to explore how fragmented compliance approaches affect employees to comply with laws, regulations and security policies regarding information in an organisation. This is conducted in order to confirm whether aspects such as governance and human factors, play any significant part in compliance, with the goal of designing a proposed integrated framework to assist in reducing non-compliance. The research underpins its findings using Neo-institutional theory, Agency Theory, Rational choice theory, as well as a framework for the governance of information security proposed by Von Solms (2004) and an organisational culture model by Denison (Denison *et al*., 2004).

## 4.2 The case

The research is based on a case study at a financial services organisation. The organisation has strict rules and regulations which requires the organisation to comply at all times in order to do business in the financial sector. The potential risk of non-compliance is a cause for concern and thus, the organisation must proactively find ways of reducing this risk.

Twenty one participants are selected and interviewed at all levels of the organisation in Cape Town, South Africa. Participants includes employees who have access to the IT network. They are divided into job level categories which is split into senior, middle and lower level employees. Of these, four senior level participants included heads of departments and senior management. As far as middle level participants are concerned, 14 are included as specialists, who hold a tertiary education and

three lower level participants with no tertiary education. They are further grouped into department levels so that the researcher can obtain a clear view to identify and find specific problem areas in the organisation. Departments included were the Finance, Research, IT, Administration, Human Resources (HR), Legal, Marketing and Sales.

In this organisation there are two departments which are responsible for information compliance namely the Technology and the Compliance Department. They work together to keep the information of the organisation safe and secure. However, there is a gap between these processes as the human factor is not properly addressed in the policies of the two departments. The two departments have no control over employees leaking information, or the unintentional breaches of information security. Another raising concern is that there is no way of tracking whether employees are in fact complying with information laws and regulations. The organisation only addresses these issues when security breaches occur and this could potentially lead to damaging consequences in future. There is an urgent need to comply to laws and regulations as the financial services industry is highly regulated.

### 4.3 The Findings

This section describes the results obtained from the interviews. The findings are presented in the following way:

i) The main research question is presented
ii) The sub-research questions follow.
iii) Under each subresearch questions, the interview question and findings are presented.
iv) The findings of the interview questions are divided into 2 levels namely;
   a) job level where the answers are explored from a senior, middle and low level position.
   b) department level examines how the departments on its own view compliance within the company.

### 4.3.1 RQ 1: What factors do organisations face in order to comply with laws, regulations and information security policies?

#### 4.3.1.1 RSQ 1.1: What are the information security compliance approaches that financial services organisations deploy?

IQ 1.1.1 Do the FSB and government ensure that your organisation complies with regulations?

**Job Level**

Of the participants, 19 out of 21 know that the organisation has to comply with regulations from either, government or a regulatory body such as, the Financial Services Board (FSB). The participants who do not know, are lower level employees that are not aware of, or do not need to know other business operations in the organisation. Interviewee 7 (lower level employee) states: ”I have no idea.” (Appendix 2). Senior and middle level employees are all aware of the part the regulator and government play in the organisation - they even have some influence on its operations for example, Interviewee 11 states: “Yes, the financial industry is constantly regulated to ensure best practices.” (Appendix 2).

**Departments**

Of the 9 departments, there are no specific departments that presents any lack of awareness of whether the FSB or government, influences compliance in the organisation. For example, Interviewee 6 states: “Yes, in order to ensure that we behave in a fit and proper manner and treat customers fairly.” (Appendix 2). The Marketing as well as Administration departments, are the only 2 departments that have 2 employees respectively, who are unclear whether the FSB or government are influencing the compliance within the organisation. Interviewee 4 simply answers: “I don’t know, because I’m not involved in that part of the business.” (Appendix 2).

Finding 1: The majority of employees know that the FSB and government ensures the organisation to comply with regulations.

IQ 1.1.2 Do you have specific corporate compliance strategies?

**Job Level**

Of the participants, 11 of the 21 know that their organisation has some or other compliance strategies which the organisation uses to reduce risk. All senior level participants are aware of the compliance approaches and strategies as Interviewee 15 states: “Yes, we have many like FICA and FAIS. We also employ a compliance officer to assist us in this regard.” (Appendix 2). However, it is found that 50% of the employees in the middle level are unaware of the compliance approaches and strategies. Interviewee 4 summarises this by stating: “I don’t know.” (Appendix 2). Some employees (3 out of 21) know that their organisation have these approaches and strategies but do not know about the approaches and strategies specifically. Interviewee 2 is more specific and says: “I think FAIS and other compliance approaches are used.” (Appendix 2). The 3 lower level Interviewees are unaware of the strategies as Interviewee 5 says: “I don’t know really, not involved in strategy making” (Appendix 2). The attitude of the middle to lower level participants is that they do not know what the strategies are mainly because if it does not affect them directly, they do not need to know. For example, IinteIntervieweenterviewee 17 states: “I don’t know I’m not a part of it.” (Appendix 2). These observations suggest that the lack of awareness amongst employees could be a potential risk issue.

**Departments**

Of the participants, 10 out of 21 who are unaware of any compliance approaches or strategies, come from the administration, finance, HR and marketing departments. Interviewee 14 says: “I wouldn’t know, hey, I was never told.” (Appendix 2). On the other hand, Interviewee 16 states that “Yes we do, and FICA is one of them.” (Appendix 2). This demonstrates the assumptions that participants have, and could be caused by communication or training issues within the organisation, as the answers are not specific to departments, but linked to job levels. It is noted that although the senior levels of these 3 departments know the strategies and approaches, at a middle and lower level in these departments, it is not the case as they are unaware of compliance strategies and approaches.

Finding 2: Half (50%) of the middle to lower level employees do not know the organisation compliance strategies.

Finding 3: All of the senior level employees know that the organisation has compliance strategies.

Finding 4: Middle and lower level employees in 3 departments do not know about the compliance strategies and approaches, despite the fact that the senior level employees are knowledgeable about these strategies.

IQ 1.1.3 In your opinion how well are your information security policies enforced?

**Job Level**

According to most (19 out of 21) of the participants across job levels, indicate that information security policies are enforced fairly well in their organisation. Interviewee 8 says: “We have adequate cover as we have not had any breach in security as yet.” (Appendix 2). Almost all (95%) of the Interviewees convey confidence in some way for policies to be enforced. The answers are in contrast to IQ 1.1.2, where the findings are presented in that middle and lower level employees do not know about the compliance strategies. These participants do not know that the information security policies form part of the organisations compliance strategies. This is amplified by Interviewee 17 saying that in the previous question IQ 1.1.2, that he does not know however, for this question answered: “In my opinion I think good.” (Appendix 2). It appears that interview question 1.1.2 may have been misinterpreted or it is unclear. Going back to some of the participants again and asking the two questions again, many (8 out of 21) think the two questions are different and that although they may not know the strategies, they do know that compliance security is in place and being enforced.

**Departments**

The answers are similar across departments and not one department stands out. While many (18 out of 21) of the participants exhume confidence in the enforcement of the organisations security policies, a few (3 out of 21) do not know what the security policies compromises of, and can not elaborate on examples of guidelines with 2 participants being from the administration department. Interviewee 11 states:

“Very well, no information is disclosed unless consent has been given by the client.” (Appendix 2). The answer is vague on distinguishing between security policies, regulation and legislature and when asked to elaborate the Interviewee can not go into further detail. Information security policies are for employees accessing, transforming and disseminating the organisation’s information and are managed by the Information Technology department. Although the information security policies are not enforced by external pressures it forms part of the organisation’s compliance strategies.

Finding 5: Employees state that information security policies are well enforced.
Finding 6: Some employees although they experience that security policies are enforced do not know what the policies strategies entails.
Finding 7: Administration department shows least knowledge about compliance strategies.

IQ 1.1.4 Does your organisation comply with regulations because of industry standards?

**Job Level**

The answers of senior level participants are split down the middle on this question. Some senior participants (2 out of 4) believe that industry standards have some influence in complying with regulations. Interviewee 16 says: “Yes we have to keep up with industry in order to remain competitive.” and Interviewee 3 states: “I don’t think so, we comply in order to protect our clients and to be able to operate in the industry.” (Appendix 2). According to Interview 15, industry standards do have an influence but there are other factors involved. Interviewee 15 states: ”Not only because of industry standards but it is one of the reasons and it does have some influence.” (Appendix 2). Some middle level participants are unable to answer, while 50% of them do not know the reasons for complying for example, Interviewee 4 says: “I’m not sure what the specific reason for complying with the regulator is.” (Appendix 2). and a few (2 out of 14) answers in the positive as well, but areunable to give any insight on the matter. All lower level employees (3 out of 30) do not know

and answers as Interview 17 states: “I don’t know, never came across or seen any evidence so I am not able to give an answer.” (Appendix 2).

**Departments**

The responses to the questions are not department specific and all of the departments have participants either, not knowing or saying industry standards is not a cause of complying. The Administration department shows the largest number (3 out of 5) of participants stating that industry standards do not have an influence on the organisation to comply. All participants in the Legal and Sales departments suggest that industry standards do have some influence in compliance and is needed for the organisation to keep up with competitors.

Finding 8: Half (50%) of senior level employees believe industry standards do not have a significant influence on compliance.

Finding 9: Half (50%) of the middle level employees do not know whether industry standards in the financial services sector do have an influence on compliance.

Finding 10: The Administration department has the highest number of employees who do not know whether industry standards have an influence on the organisations compliance endeavours.

#### 4.3.1.2 RSQ 1.2: What are the challenges financial services organisations face in order to comply with the regulatory body’s laws and guidelines?

IQ 1.2.1 Are you aware of the major factors considered in complying with the regulator?

**Job Level**

As expected, senior management are aware of the major factors involved in complying with the regulator. Interviewee 15 indictaes that a major factor is “Accurate information.” (Appendix 2). Many (10 out of 14) of the middle level participants know the major factors which includes factors such as, complete information, fraudulent behaviour, money laundering and is stipulated by the regulator. A few participants on middle level (30%) do not know what the major

factors are as Interviewee 19 states “I don’t know, I don’t deal with the regulator.” (Appendix 2). Lower level employees can not mention any factors considered in complying with Interviewee 20 saying “I don’t really know, it’s never been communicated to me.” (Appendix 2).

**Departments**

Administration, finance and marketing are the departments with the least knowledgeable participants. Interviewee 10 says “I’m not sure. I don’t deal with the regulator.” (Appendix 2). This could be because these departments have less communication with the regulator than the other departments. Participants from Sales and Legal are the most knowledgeable for example, Interviewee 6 from Sales answers that the regulator requires them “Behaving in a fit and proper manner, treating customers fairly and information security and confidentiality.” (Appendix 2). Interviewee 18 states that “Major factors would be making sure you follow everything by the book and comply or else we would be penalized. We could face heavy fines by not complying.so we have to follow everything by the book.” (Appendix 2).

Finding 11: Most of the participants know about what the factors considered in complying with regulations are.

Finding 12: All employees in the Sales and Legal department know what the factors considered are, when complying with the regulator.

Finding 13: The main factors that need to be considered when complying with the regulator are complete and accurate information, fraudulent behaviour and money laundering.

Finding 14: Senior level participants are more aware of which factors are considered in complying with regulations.

IQ 1.2.2 Are you aware of any challenges you are experiencing when facing these factors in an attempt to comply?

**Job leve**l

The senior level participants are aware of the challenges and are able to specify challenges as Interviewee 16 says “Having all the information available during audits

is one of the challenges they face as it becomes deadline driven." (Appendix 2). Interviewee 9 states: "Accurate information that is readily available." (Appendix 2). Middle and lower level employees are found to be the least aware (7 out of 17). Interviewees do not know the challenges they face when complying while more than 50% give different challenges that they experience. The challenges are widespread with no common denominator. Interview 18 states: "It's challenging in the sense that everything has to be by the book, but I'm already groomed into this mindset and apply as far as I can. My challenge is to keep myself up to date with the latest regulations." Interviewee 21 says that "…enhancing the system to accommodate regulations in a very short period of time.", to be the main challenge (Appendix 2). Interviewee 12 states that one of the factors he finds challenging is that "Consumers aren't always truthful with their information." (Appendix 2). Many of the participants mention the lack of information and availability of information as well as that incomplete, inaccurate information underpins the challenges they face in complying. Senior level employees also agree that information is one of the greatest challenges.

**Departments**

As in the question asked before, The Sales and Legal department together with senior management are found to have the strongest views. The participants answers more in-depth and are able to specify exactly where the challenges are in complying. Interviewee 15 states: "Submitting the right information and abiding by regulations that affect our business." (Appendix 2). Other departments such as Administration, Finance and Marketing have the weakest responses with many answering that they do not know what the challenges are in complying. Interviewee 17 states: "I'm not completely sure and can't say exactly." (Appendix 2).

Finding 15: Senior level employees, the sales and legal department have the strongest awareness of the challenges facing the organisation.

Finding 16: Middle to lower level participants are less aware of challenges facing the company when complying with the regulator's demands.

IQ 1.2.3 How do you overcome the challenges you are facing?

**Job Level**

Senior level participants know how to overcome the challenges. Interviewee 15 says that “With the assistance of Information Systems and the implementation of better business processes they try to overcome some of the challenges they face.” (Appendix 2). A quarter (25%) which relates to (5 out of 21) of the participants do not know how to overcome their challenges to comply while 75% (16 out of 21) of the participants, use different methods respectively to overcome challenges. However they find no proper guidelines in place that have been communicated to everyone in order to deal with the challenges as Interviewee 11 states: “Gathering information, finding out the source of funds etc are major challenges.” (Appendix 2) and Interviewee 12 responds that “We need to have better guidelines in place in order to validate consumers’ information.” (Appendix 2). It appears as if there is a communication issue from senior through to lower level employees, as senior level employees all know how to overcome challenges. This however, breaks down as the job level decrease.

**Departments**

Senior level and the Sales department are found to be the strongest in managing the challenges. Most participants (16 out of 21) are aware of what to do while some middle to lower level employees (5 out of 21) are found to be weaker with many inconsistencies in the answers of participants as Interviewee 10 states: “I take it up with my manager.”, and Interviewee 14 says “Aim to get the most accurate information we possibly can.” (Appendix 2).

Finding 17: There is no structure or guidelines to follow when employees face challenges to comply.

Finding 18: Senior level and the Sales department are more aware of how to deal with challenges in order to comply.

Finding 19: Middle to low level have inconsistent answers and do not know how to manage challenges as and when they occur.

### 4.3.2 RQ2: How does the information security culture influence compliance to information security policies and regulations?

#### 4.3.2.1 RSQ 2.1: How does governance influence information security compliance?

IQ 2.1.1 Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security?

**Job Level**

All senior level participants agree that the consumer and stakeholders expectations do influence compliance. Interviewee 16 supports this by saying “Yes, that is another reason we have to comply so that our clients can trust us with their money.” (Appendix 2). A few participants (2 out of 21) are of the opnion that it is not the only reason they have comply as some stakeholders do influence the organisation while many of the participants (17 out of 21) answers, that consumer and stakeholder expectations do influence compliance in a good way. Interviewee 14 says “We must ensure that the consumer feels safe enough to trust us.” (Appendix 2). Middle level participants confirm that consumer expectations for their financial and personal information are to be fully protected, at all times, and are of utmost importance and has a positive influence on compliance. The organisation builds up this trust with consumers by ensuring they comply with regulations and following best practices. Lower level participants are all unaware any specific reason as to why the organisation complies with regulations with Interviewee 20 saying that “I don’t really know” and Interviewee 7 states: “I have no idea.” (Appendix 2).

**Departments**

Answers are the same across all departments and there are no specific department highlighted in any way. Interviewee 21 from the legal department, states: “To my knowledge compliance is initiated from the FSB and they have privacy and security concerns to protect consumers.”, while Interviewee 14 states: “We must ensure that the consumer feels safe enough to trust us.” (Appendix 2).

Finding 20: Consumer and stakeholders expectations positively influence compliance.

IQ 2.1.2 How do regulations and policies influence your organisations information's security?

**Job Level**

All senior level participants are aware of how regulation and policies influence their organisation's information security with Interviewee 16 saying: "They positively influence it by ensuring we follow effective guidelines." (Appendix 2). All (14) middle level participants answer they believe regulations and security policies have a positive influence on information security in the organisation for example Interviewee 18 says: "It makes people think twice before they step out of line or don't follow procedures because they are aware of the implications.". Interviewee 11 states that "They increase information security in the business by restricting access to what employees can or can't do." (Appendix 2). Low level participants are unable to answer with Interviewee 7 for example, saying: "I don't know." (Appendix 2). Others either are not sure, or do not know.

**Departments**

Answers are the same across all departments and there are no specific department highlighted in any way. The answers suggests that regulations and policies have a positive influence on information security. As Interviewee 12 states: "Regulations and policies are implemented by law. Your organisation's information security needs to abide by that law in order to do business legally." (Appendix 2). The organisation is forced to abide by these regulations and policies in order for it to be legally compliant. This positively influences its information security practices.

Finding 21: Regulations and policies in the organisation have a positive influence on information security.

IQ 2.1.3 What role does management play in implementation of information security compliance?

**Job level**

Almost all (17 out of 18) of senior and middle level participants believe that its managements responsibility to enforce security policies and regulations. Interviewee 11 says that “management ensures that the correct processes are in order to comply with regulations.”, similarly, Interviewee 21 states:“…management is the driving force behind any sort of compliance.” (Appendix 2). The low level participants are all unaware of the role management plays in implementing information security compliance for example, Interviewee 17 states:“I’m not completely sure on what role they role they play.” (Appendix 2).

**Departments**

The Administration department has 2 participants who are totally unaware of the role that management plays in compliance. For example, Interviewee 20 states: “I don’t know unfortunately.” (Appendix 2). All other departments are able to answer appropriately, where Interviewee 12 says: “Management needs to ensure that all information security guidelines abides with these of the Regulator.”.

.

Finding 22: Almost all of the participants believe management is responsible for enforcing compliance in information security.

Finding 23: The Administration department and low level employees shows less knowledge about the role that management plays in enforcing compliance in the organisation.

#### 4.3.2.2 RSQ 2.2: How does employee information security knowledge influence compliance?

IQ 2.2.1 Are you regularly informed of any changes in compliance requirements?

**Job Level**

Senior and middle level making up 80% of the participants, are of the opinion that they are regularly informed about compliance changes, but only when and if they are required to know. Interviewee 12 states: “Yes, it’s the organisation’s responsibility to keep the employee up to date with any changes to compliance.” (Appendix 2). In order for the employees to comply they need to be kept up to date with any changes in requirements. Of the participants, 20% believe they are not informed of any changes about compliance requirements and this falls into middle to lower level participants, as their jobs do not require them to know. For example, Interviewee 1 states: “No, it does not form a major part of my job.”, whereas Interviewee 7 says “…sometimes, I guess it depends on what type of change it is and if I’m involved in it.” (Appendix 2).

**Departments**

The Administration department has the most Interviewees saying that they are not informed regularly, or that their job does not require them to know. All the other departments respond that they are regularly informed of changes in compliance requirements for example, Interviewee 6 says: “Yes, in order for our company to comply with new/changes to regulation.” and Interviewee 8 states: “Yes, we have regular forums where possible changes if any are discussed and decided on.” (Appendix 2).

Finding 24: Most employees are regularly informed of changes in compliance requirements.

Finding 25: Some middle to lower level employees does not know as their job does not require them to know.

Finding 26: Administration department participants were the least knowledgeable of changes in compliance requirements.

IQ 2.2.2 Are you are aware of the risk of non-compliance?

**Job Level**

All of the senior level participants are aware of the risks of non-compliance. Interviewee 16 states: “Yes I am so that I may reduce the risk of it ever happening things such as fines or penalties and in worst case in could lead to prosecution.” (Appendix 2). As expected, senior level employees know what the risks are and often get updated during senior management meetings. They are supposed to pass the information down to their respective departments. Almost half of the participants in the middle level are unaware of the potential risks of non-compliance to security policies or regulations. Interviewee 10 states: “No I don’t know I was never informed.” (Appendix 2). This is worse at the lower level where all of the participants do not know the risks of not complying with security policies and regulations. Interviewee 17 states: “No I am not, I just know that we must do it to be able to do business,” and Interviewee 20 says: “Not really. I don’t think I need to know.” (Appendix 2). This suggests that there is a gap in communication from senior level down to lower level employees. The information is not being passed down effectively and as a result, many of the middle to lower level employees are left unaware of the risks of non compliance.

**Departments**

The Finance and Administration departments are found to have the largest number of participants that are unaware of the risk not complying. Interviewee 19 from the Finance department says: “Not really, just know that it’s not good for the business.” (Appendix 2). Many of these participants know that there is some kind of consequence however, they do not know specifically, what they are.

Finding 27: Many of middle to low level participants are not fully aware of the risk for not complying.

Finding 28: Senior level participants are all aware of the risks of not complying that results in fines, penalties and prosecution.

IQ 2.2.3 What do you do when faced with information security problems?

**Job Level**

More than half (10 out of 17) of the participants from middle to lower level escalate any information security problems to their superiors as Interviewee 1 states: “I take the issue to my manager.” (Appendix 2). The other half calls on IT to assist them in dealing with any information security problems or attempt to resolve the issues themselves for example, Interviewee 12 states: “You analyse the issues and work out a plan of action to fix the issues.” (Appendix 2). There is no process of dealing with information security incidents or employees are not fully aware of the procedures to follow in such a situation. For example, Interviewee 5 states: “I’m not sure I never faced anything yet and I am not sure on the procedures to follow.” (Appendix 2).

**Departments**

Answers are the same across all departments and there are no specific departments highlighted in any way as Interviewee 1 from IT states: “I take the issue to my manager.” and similarly, Interviewee 4 from Marketing says: “I take the issue to my manager.” (Appendix 2).

Finding 29: Participants are not fully aware of how to deal with information security incidents.

Finding 30: There are no business processes to follow when dealing with information security problems.

Finding 31: Many of the participants escalate any issue to their superiors.

IQ 2.2.4 Do you access information that is not meant for you?

**Job Level**

Only one participant in the middle level admits to accessing information not meant for him (Interviewee 18) and states: “Yes I’m guilty, I have access to all the sites as well as information that is not meant for me, but I will take a look, just to know what’s happening inside the company.” (Appendix 2). One participant from the senior level

who is the Information Systems manager, accesses information that's not meant for him because it falls in his job description as he manages all the information in the organisation. Most (90%) of the Interviewees say they do not access any information that is not meant for them. It is not easy to determine if participants are completely honest answering this question as participants may think answering such questions honestly, could land them in trouble.

**Departments**

All departments indicate that they do not access information that is not meant for them. For example, Interviewee 14 states: "No, I do not if it's not meant for me." and Interviewee 12 states: "No, unless authorized to do so." (Appendix 2). There is no specific department highlighted in any way.

Finding 32: Employees do not access information not meant for them.

IQ 2.2.5 Do you know of any policies or laws that exist surrounding information?

**Job Level**

Senior level participants are aware of policies and laws that exists surrounding information as Interviewee 15 states: "Yes, FICA and the Protection of Personal Information Act is examples of such laws." (Appendix 2). A low number of participants (40%) comprising (5 out of 21) of middle to lower level are either, completely unaware or can not specify any policies or laws surrounding information. Interviewee 4 states: "No, not really, I just know that there are policies and laws." (Appendix 2). Interviewee 5 states: "Not really, I know there is just not sure what."(Appendix 2). A larger part, 60% (16 out of 21) of the participants know that there are laws and policies while some mention things that are not relevant laws. They mention laws such as plagiarism (copyright laws), protection of personal and intellectual property laws and the protection of information bill that has been brought about by the South African parliament in 2014.

**Departments**

The Administration department is found to be most unaware of laws and policies for example, Interviewee 13 states: “Not really, don’t know.” (Appendix 2). There are no other departments that stand out. The majority of participants in each department know that information is governed in some way or another.

Finding 33: Many of the employees do know that there are laws and policies surrounding information but do not necessarily know what they are.

IQ 2.2.6 Who is responsible for the security of your organisations information?

**Job Level**

Of the participants, 75% amounting to 16 out of 21 and ranging from senior to lower level indicate it is solely the responsibility of the IT department for the security of the organisation’s information. Interviewee 12 states: “That would be the employees responsible for maintaining the information server such as IT.” (Appendix 2). Interviewee 2 says it “…is the responsibility of the compliance department.” (Appendix 2). Similar answers are given by most (16 out of 21) of the participants all saying it is the responsibility of IT. Not enough motivation is displayed from participants to protect the information of the organisation. They are not aware that they are also responsible for the security of information in the organisation.

**Departments**

Most of the departments answers are in consensus, saying that IT is responsible for the security of the information for example, Interviewee 3 and 6 say “IT.” (Appendix 2). Some employees (2 out of 21) say that it is management as Interviewee 5 states: “Probably senior management.,”. Two participants from the IT department state: “Compliance officers.” and “My manager and team.”, respectively (Appendix 2). There is no common department highlighted in any way.

Finding 34: Most of the participants believe IT is solely responsible for the organisations information.

Finding 35: Many of the participants believe information security is not their responsibility.

#### 4.3.2.3 RSQ 2.3: How does information security compliance affect employee performance?

IQ 2.3.1 Do you think observing, tracking and notification of security incidences are part of your daily work routine?

**Job Level**

One of the senior level participants finds that monitoring and reporting security incidences is not part of their daily routine. However, Interviewee 15 states: “No not really but when an incident does occur we deal with it immediately.” (Appendix 2). Most (3 out of 4) of the senior level participants agree it does form part of their daily routine as Interviewee 16 states: “Yes it does in order to reduce the risk of it which falls under my responsibilities.” (Appendix 2). Many middle level participants, up to 50% (7 out of 14) say it does not form part of their daily routine. Interviewee 13 states: “There are enough security controls I think.” (Appendix 2). Similarly, Interviewee 8 mentions that “It is not part of my routine as it’s managed through our IT department.” (Appendix 2). This can be deemed a potential security risk as many middle level employees are not involved in monitoring and reporting security incidents. There are a few (3 out of 14) middle level participants who answer that it is not a daily routine, but they do report it if the need arises. All of the lower level participants responds that it does not form part of their daily work routine, as Interviewee 20 states: “No I don’t think so I’m not sure.” (Appendix 2).

**Departments**

The answers are interesting for further analyses, as all the departments have participants split between both, monitoring and reporting their security incidents. Many of the participants who indicate they do not track, observe or notify security incidents in their daily routine, also state that they do bring security incidents to light when such security incidents arise. One participant of the IT department answers that they do not track, notify or observe security incidents for example, Interviewee 2

argues: “No, I am a Business Analyst in Information Systems so it’s part of my responsibilities.” (Appendix 2).

Finding 36: The tracking and reporting of security incidences are not done on continuous basis exposing the organisation to security breaches.
Finding 37: Information security processes are not included into employee’s daily routine.

IQ 2.3.2 In your opinion does complying with policies and regulations hamper your productivity?

**Job Level**

All senior level participants answer that complying with policies and regulations does not hamper their productivity. Half of the participants from the middle level indicate complying does hamper their productivity. Interviewee 12 states: “Yes, because it limits your interaction with the information at stake.” (Appendix 2). Half of the middle level participants (7 out of 17), find while it does hamper their productivity, it is a requirement in their job role. For example Interviewee 19 says “Yes it does but it’s necessary.” and Interviewee 14 states: “Yes it does but we must do it to comply.” (Appendix 2). All of the lower level participants say it does not hamper their productivity as Interviewee 17 states: “No I don’t believe so.” (Appendix 2).

**Departments**

The Sales, Finance and Marketing departments are found to be more inclined to think that complying to policies and regulations hampers their productivity. For example, Interviewee 12 from the Marketing department, states: “Yes, because it limits your interaction with the information at stake so we might not be able to finish a task sooner because of certain processes that needs to be followed.” (Appendix 2).

Finding 38: Half of the middle level participants believe complying with security policies and regulations hampers their productivity.
Finding 39: Senior and lower level participants believe complying with policies and regulations does not hamper their productivity.

#### 4.3.2.4 RSQ 2.4: How do organisations manage the potential reputational damage that fragmented compliance approaches create?

*IQ 2.4.1 Do you think protection of information is part of the organisation's strategy?*

**Job level**

All the senior level participants respond that it is part of the organisation strategy to protect information as Interviewee 16 states: "Yes. our information is very important and it must be protected." (Appendix 2). Most (11 out of 14) of the middle level participants believe that protection of information forms part of the organisations strategy. Interviewee 12 states: "Yes, they need to ensure that information is protected, because they can get sued if information has been corrupted or leaked." (Appendix 2). Many lower level participants (2 out of 3) do not know, while a middle level participant Interviewee 13 is of the opinion that the protection of information is not part of the strategy. While most people agree that the protection of information is part of the organisation's strategy, some of the participants are uncertain and the uncertainty of participants suggest that middle to lower level employees are excluded from any information strategies and goals the organisation may have.

**Departments**

Although the senior level employees in the Administration, Finance and HR departments know that the protection of information is part of the organisational strategy, middle and lower level employees are uncertain that the organisations strategy includes the protection of information in any way. The other departments such as, Legal are of the opinion that information protection forms part of their business strategy for example, Interviewee 18 states: "Of course, especially ours because we have so many competitors that we don't want our information leaked out too, this is what sets us apart from our competitors. We are unique in our policies and strategies which is highly confidential." (Appendix 2).

Finding 40: Senior level participants know that the protection of information is part of the organisation strategy.

Finding 41: Some middle to lower level participants are excluded from information strategies or goals of the organisation.
Finding 42: Administration, Finance and HR are uncertain whether the organisation strategy included protecting information.

*IQ 2.4.2 Do you think the organisation evaluates past security experiences?*

**Job level**

Senior and middle level participants are of the opinion that the organisation does evaluate past security experiences. Interviewee 1 states: “Yes, because they use this experience to better their security.” (Appendix 2). Similar answers are received from the participants all saying that they do evaluate past security experiences in order to learn and improve. Interviewee 12 states: “Yes, that is how an organisation would improve on its securities and regulations.” Interviewee 4 states: “Yes I do think so, so that they can fix errors of the past so that it don’t happen again.” (Appendix 2). Of the participants, 2 out of 3 lower level participants are unaware of the evaluation of past security experiences.

**Departments**

Most of the answers received conclude that the organisation does evaluate past experiences as Interviewee 18 from the legal department says: “Yes all the time, we always have a review of past experiences, sometimes to see what we can improve on and what we can still keep, we are big on this notion and have constant meetings around this.” Interviewee 16 responds: “Yes we do in order to mitigate our risks.” (Appendix 2). Interviewee 5 from Finance did not know and says: “Im not sure, never heard of it yet.” (Appendix 2).

Finding 43: Senior to middle level participants are of the opinion that the organisation evaluates past experiences to reduce the risk of it happening again.
Finding 44: Lower level participants unware if the organisation evaluates past security experiences.

*IQ 2.4.3 Does your organisation have a data backup and disaster recovery plan?*

**Job Level**

Most (19 out of 21) of the participants across senior to lower level participants agree that they do have a backup plan and confirm to have a DR off site. Interviewee 2 states: “Yes, backup to ensure that we can roll back anytime. Disaster recovery is in place for business continuity during disasters.’ Interviewee 20 responds: “Yes I believe we have a DR offsite for that.” (Appendix 2). This is important and forms part of regulations in large organisations and proper planning around information assets substantially reduces risk.

**Departments**

All departments know that their organisation has some kind of disaster recovery and data backup plan.

Finding 45: The employees are aware that the organisation has a disaster recovery and backup plan.

IQ 2.4.4 Are risk vulnerability checks constantly conducted in your organisation?

**Job level**

Senior level participants find that risk vulnerability checks are done regularly in the organisation. Interviewee 16 states: “Yes, we perform them regularly.” (Appendix 2). Half of the participants in the middle level confirm there are risk vulnerability checks conducted in the organisation while the other 50%, are of ther opinion they are either, not aware of it, or they do not know. Interviewee 10 states: “I don’t know or never heard of it.” (Appendix 2). Ensuring employees are aware that checks are done on a regular basis plays an important role in protecting information. Interviewee 5 also confirms that: “Not that I’m aware of.” (Appendix 2). Lower level participants are all unaware and answers that they do not know. For example, Interviewee 7 states: “I don’t know.” (Appendix 2).

**Departments**

The Administration department has the most participants who are unaware if any risk vulnerability checks are done inside the organisation. Interviewee 17 states: “I wouldn’t know hey.”, and Interviewee 13 exclaims: “I’m not sure.” Both, belong to the administration department (Appendix 2).

Finding 46: Middle level participants are not fully aware if vulnerability checks are conducted in the organisation.

Finding 47: All lower level participants do not know if any checks are done.

Finding 48: All senior level participants said that there are risk vulnerability checks done within the organisation.

IQ 2.4.5 Is creating user awareness on security threats part of education and training in the organisation?

**Job level**

All senior level participants agree that user awareness on security threats are a part of training and education within the organisation.Interviewee 15 states: “Yes, we give our employees training in our induction program.” (Appendix 2). Some,(5 out of 14) middle level participants suggest that creating user awareness and training is not ongoing, and that they only receive training upon arrival in the induction programme, and then never again. They suggest that there is no continuous educating of users on security threats. Interviewee 13 states: “No, only when and if a security incident happens would we be told about it.” (Appendix 2). The biggest threat is found to be in the lower level employees. Training is not ongoing and new threats are created every day. Lower level participants all say they are not given proper ongoing training with Interviewee 20 stating: “No, I think ongoing training is only for certain people.” (Appendix 2). Employees need to be kept up to date and trained to be aware of potential threats before it happens.

**Departments**

The Administration department is unaware of training and education on potential security threats as Interviewee 10 from the Administration department states: “We

get induction when we start to make us aware." and Interviewee 17 also from the Administration department states: "No we never do training on it." (Appendix 2).

Finding 49: Many of the participants in middle to lower level only receive security threat management training at the induction when joining the company and no training thereafter.
Finding 50: Senior level participants all receives ongoing training and education on potential security threats.
Finding 51: Administration department do not give ongoing training on security threats.

## 4.4 Summary of the findings

Table 4.1 depicts a summary of all the interview questions and findings. It further depicts the job level and departments that responded negatively to the interview questions. This contents can be used to determine where the challenges and risks are for the organisation.

**Table 4.1: Summary of findings**

| Questions | Findings | Job Level - Not in agreement | Department- Not in agreement |
|---|---|---|---|
| **RQ 1: What are the factors that influence compliance to information security policies and regulations?** | | | |
| **SRQ 1.1 What are the information security compliance approaches that financial services organisations deploy?** | | | |
| IQ 1.1.1) Do the FSB and government ensure your organisation complies with regulations? | Finding 1: The majority of employees said that the FSB and government do ensure that organisation complies with regulations. | Lower level | Marketing & Admin |
| IQ 1.1.2) Do you have specific corporate compliance approaches/strategies? | Finding 2: Half of the middle to lower level employees does not know the organisations compliance approaches or strategies. | Middle and Lower level | Admin, Finance, HR, Marketing |

| | | | |
|---|---|---|---|
| | Finding 3: All of the senior level employees know that the organisation has compliance approaches and strategies. | | |
| | Finding 4: Middle and lower level employees in 3 departments do not know about the compliance strategies and approaches despite the fact that the senior level employees are knowledgeable on the strategies. | | |
| IQ 1.1.3) In your opinion how well are your information security policies enforced? | Finding 5: Employees state that information security policies are well enforced | None | None |
| | Finding 6: Some employees although they experience that security policies are enforced do not know what the policies entails. | | |
| | Finding 7: Administration department shows lease knowledge about compliance strategies | | |
| IQ 1.1.4) Does your organisation comply with regulation because of industry standards? | Finding 8: Half of senior level employees believe industry standards do not have a significant influence on compliance | Middle & Lower Level | None |
| | Finding 9: Half of the employees do not know whether industry standards in the financial services sector do have an influence on compliance. | | |
| | Finding 10: Administration department has the most amount of employees who do not know whether industry standards has an influence on compliance | | |
| **SRQ 1.2 What are the challenges financial services organisations face in order to comply with the regulatory body's laws and guidelines?** | | | |
| IQ 1.2.1) What are the major factors | Finding 11: Most of the | Lower Level | Admin, Finance |

| | | | |
|---|---|---|---|
| considered in complying with the regulator? | participants know about what factors considered in complying with regulations were | | and Marketing |
| | Finding 12: All employees in the Sales and Legal department know what the factors considered when complying with the regulator | | |
| | Finding 13: The main factors that need to be considered when complying with the regulator are complete and accurate information, fraudulent behaviour and money laundering. | | |
| | Finding 14: Senior level participants are more aware of which factors are considered in complying with regulations | | |
| IQ 1.2.2) Are you aware of any challenges you are experiencing when facing these factors to an attempt to comply? | Finding 15: Senior level employees, the sales and legal department found to have the strongest awareness of the challenges facing the organisation | None | Admin, Finance and Marketing |
| | Finding 16: Middle to lower level participants are less aware of challenges facing the company when complying. | | |
| IQ 1.2 3) How do you overcome the challenges you are facing? | Finding 17 There is no structure or guidelines to follow when employees face challenges to comply. | Middle & Lower Level | None |
| | Finding 18: Senior level and Sales department found to be more aware on dealing with challenges to comply | | |
| | Finding 19: Middle to lower level have inconsistent answers and do not know how to manage challenges as and when they occur. | | |
| **RQ 2: How does the information security culture influence compliance** | | | |

| | | | |
|---|---|---|---|
| **to information security policies and regulations?** | | | |
| **SRQ 2.1 How does governance influence information security compliance?** | | | |
| IQ 2.1.1) Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security? | Finding 20: Many of the participants believe consumer and stakeholders expectations positively influence compliance | Lower Level | None |
| IQ 2.1.2) How do regulations and policies influence your organisations information's security? | Finding 21: Regulations and policies in the organisation has a positive influence on information security. | Lower Level | None |
| IQ 2.1.3) What role does management play in implementation of information security compliance? | Finding 22: Almost all of the participants believe management is responsible for enforcing compliance in information security | Lower Level | Admin |
| | Finding 23: The Administration department shows less knowledge than other departments. | | |
| **SRQ 2.2 How does employee information security knowledge influence compliance?** | | | |
| IQ 2.2.1) Are you regularly informed of any changes in compliance requirements? | Finding 24: Most employees are regularly informed of changes in compliance requirements. | None | Admin |
| | Finding 25: Some middle to lower level employees does not know as their job does not require them to know. | | |
| | Finding 26: Administration department participants were the least informed of changes in compliance requirements. | | |
| IQ 2.2.2). Are you are aware of the risk of non-compliance? | Finding 27: Many of middle to low level participants are not fully aware of the risk in not complying. | Middle & Lower Level | Admin & Finance |

| | | | |
|---|---|---|---|
| | Finding 28: Senior level participants are all aware of the risk in not complying. | | |
| IQ 2.2.3) What do you do when faced with information security problems? | Finding 29: Participants are not fully aware of how to deal with information security incidents. | Middle & Lower Level | None |
| | Finding 30: There are no business processes to follow when dealing with information security problems. | | |
| | Finding 31: Many of the participants escalate any issue that arise to their superiors. | | |
| IQ 2.2.4) Do you access information that is not meant for you? | Finding 32: Employees do not access information not meant for them | None | None |
| IQ 2.2.5) Do you know of any rules or regulations that exist around information? | Finding 33: Many of the employees do know that there are laws and policies surrounding information but do not necessarily know what they are. | Middle & Lower Level | Admin |
| IQ 2.2.6) Who is responsible for the security of your organisations information? | Finding 34: Most of the participants believe IT is solely responsible for the organisations information. | None | None |
| | Finding 35: Many of the participants believe information security is not their responsibility. | | |
| **SRQ 2.3 How does information security compliance affect employee performance?** | | | |
| IQ 2.3.1) Do you think observing, tracking and notification of security incidences are part of your daily work routine? | Finding 36: The tracking and reporting of security incidences are not done on continuous basis exposing the organisation to security breaches. | Middle & Lower level | None |
| | Finding 37: Information security processes are not included into employee's daily routine. | | |

| | | | |
|---|---|---|---|
| IQ 2.3.2) In your opinion does complying with policies and regulations hamper your productivity? | Finding 38: Half of the middle level participants believe complying with security policies and regulations hampers their productivity. | None | Sales, Finance & Marketing |
| | Finding 39: Senior and low level participants believe complying with policies and regulations does not hamper their productivity. | | |
| **SRQ 2.4 How do organisations manage the potential reputational damage that fragmented compliance approaches create?** | | | |
| IQ 2.4.1) Do you think protection of information is part of the organisation's strategy? | Finding 40: Senior level participants know that the protection of information is part of the organisation strategy. | Middle & Lower Level | Admin, Finance & HR |
| | Finding 41: Middle to lower level participants are excluded from information strategies or goals of the organisation. | | |
| | Finding 42: Administration, Finance and HR are uncertain whether the organisation strategy included protecting information | | |
| IQ 2.4.2) Do you think the organisation evaluates past security experiences? | Finding 43: Senior to middle level participants are of the opinion that the organisation evaluates past experiences to reduce the risk of it happening again. | Lower Level | None |
| | Finding 44: Lower level participants unware if the organisation evaluates past security experiences. | | |
| IQ 2.4.3) Does your organisation have a data backup and disaster recovery plan? | Finding 45: The employees are aware that the organisation has a disaster recovery and backup plan | None | None |
| IQ 2.4.4) Are risk vulnerability checks constantly conducted in your | Finding 46: Middle level participants are not fully aware if | Lower Level | Admin |

| | | | |
|---|---|---|---|
| organisation? | vulnerability checks are conducted in the organisation.<br><br>Finding 47: All lower level participants do not know if any checks are done.<br><br>Finding 48: All senior level participants said that there are risk vulnerability checks done within the organisation. | | |
| IQ 2.4.5) Is creating user awareness on security threats is part of education and training for the organisation? | Finding 49: Many of the participants in middle to lower level only receive security threat management training at the induction when joining the company and no training thereafter.<br><br>Finding 50: Senior level participants all receive ongoing training and education on potential security threats.<br><br>Finding 51: Administration and the HR department not given ongoing training on security threats | Middle & Lower Level | Admin |

The findings identifies problem and strength areas affecting information security compliance in the organisation. The summarised findings in Table 4.1 depicts that the Administration department is least aware of the information security compliance requirements of the organisation, followed by the Finance and Marketing departments.

Middle to lower level employees are found to pose a threat to information security compliance with lower level employees being highlighted as the biggest threat. Most of the lower level employees have little or no knowledge of compliance objectives and goals. Senior level employees are found to be most knowledgeable and pose no threat to information security compliance.

By applying thematic analysis, themes are derived from the findings, linked to the interview questions, and interview questions are in turn, linked to the sub research questions. The relevant theories which apply to the organisation are also linked to themes. Headline findings derived from the findings are linked to each construct of the given theory. The linkages can be observed in Table 4.2. The following themes are developed: i) compliance and regulations, ii) risk, strategy, responsibility and security control and iii) knowledge, communication, training and productivity.

**Table 4.2: Linkage between theory, framework constructs, factors affecting information security, interview questions, findings and themes**

| Framework/ Theory | Framework construct | Factor | Interview Question | Finding | Headline Finding | Theme |
|---|---|---|---|---|---|---|
| Neo- Institutional Theory | Coercive isomorphism | Regulatory pressure | IQ1.1.1, IQ2.1.2 | Finding 1, Finding 21 | Regulatory pressure has a positive influence on information security governance | Compliance, Regulations |
| | Normative isomorphism | Client and Stakeholder pressure | IQ2.1.1 | Finding 20 | Internal and external stakeholder pressure has a positive influence on information security governance | Knowledge |
| | Mimetic isomorphism | Industry pressure | IQ1.1.4 | Finding 8 Finding 9, Finding 10 | Industry pressure has little to no influence on information security governance | Knowledge |
| A framework for the governance of information security by von Solms (2004) | Governance | External risks | IQ1.2.2 | Finding 15, Finding 16 | Information security governance has a positive influence on compliance with information security policies and regulations | Risk |
| | | Internal risks | IQ1.2.2 | Finding 15, Finding 16 | | |
| | | Strategy | IQ1.1.2, IQ2.4.1 | Finding 2, Finding 3, Finding 4, Finding 40, Finding 41, Finding 42 | | Strategy |
| | | Vision | IQ1.1.2 | Finding 2, Finding 3, Finding 4 | | |
| | | Mission | IQ2.2.1 | Finding 24, Finding 25, finding 26 | | |
| | | Policy | IQ1.1.3, IQ2.1.2 | Finding 5, Finding 6, Finding 21 | | Regulations |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Management | IQ2.1.3 | Finding 22, Finding 23 | | Responsibility |
| | | Legal/Regulatory | IQ2.1.2 | Finding 21 | | Regulations |
| | | Business issues | IQ1.2.1 | Finding 11, Finding 12, Finding 13, Finding 14 | | Knowledge |
| | | Standards | IQ1.2.3, IQ2.2.3 | Finding 17, Finding 18, Finding 19, Finding 29, Finding 30, Finding 31 | | Training, Security Control |
| Denison's organisational culture model (Denison *et al*., 2004). | Culture | Mission – Strategic Direction and Intent, Goals and Objectives and Vision | IQ1.1.2, IQ2.2.1, IQ2.2.6, IQ2.4.1 | Finding 2, Finding 3, Finding 4, Finding 24, Finding 25, Finding 26, Finding 34, Finding 35, Finding 40, Finding 41, Finding 42 | Information security culture has a positive influence on compliance with information security policies and regulations | Strategy |
| | | Adaptability – Creating Change, Customer Focus and Organisational Learning | IQ2.2.1, IQ2.2.2, IQ2.2.5, IQ2.3.1, IQ2.3.2, IQ2.4.5 | Finding 24, Finding 25, Finding 26, Finding 27, Finding 28, Finding 33, Finding 38, Finding 39, Finding 49, Finding 50. Finding 51 | | Communication, Knowledge, Responsibility, Productivity, Training |
| | | Involvement - Empowerment, Team Orientation and Capability Development | IQ2.1.3, IQ2.2.2, IQ 2.2.3, IQ2.2.6 | Finding 22, Finding 23, Finding 27, Finding 38, Finding 29, Finding 30, Finding 31, Finding 34, Finding 36 | | Responsibility, Knowledge Security Control |
| | | Consistency – Core Values, Agreement, Coordination/Integration | IQ2.2.3, IQ2.2.4, IQ2.3.1, IQ2.4.2, IQ2.4.3, IQ2.4.4 | Finding 29, Finding 30, Finding 31, Finding 32, Finding 43, Finding 44, Finding 36, Finding 37, Finding 45, Finding 46, Finding 47, Finding 48 | | Security Control, Responsibility, Risk, Productivity |

## 4.5 Summary

The findings highlight the factors influencing information security compliance as well as the strengths and weaknesses in information security compliance behaviour. Potential risks such as low awareness and knowledge regarding information security compliance are found in lower level employees and in the Administration

department. Senior level employees are found to pose the least risk and are strong in knowledge and awareness, when complying to information security compliance.

Headline findings include regulatory and stakeholder pressure to have a strong influence on information security compliance, while industry pressure has little influence. Information security governance and organisational culture are also found to have strong influence on information security compliance in the organisation. The themes developed from the findings include i) compliance and regulations, ii) risk, strategy, responsibility and security control and iii) knowledge, communication, training and productivity.

The following Chapter deals with the research themes of the research. Chapter 5 also includes the discussion of themes, headline findings, the proposed framework and conclusions.

## 5. Discussion and conclusions

### 5.1 Introduction

This chapter focusses on the discussion of themes identified in the previous chapter dealing with the findings of analysed data, collected from participants. This chapter also includes the discussion of headline findings, presents a proposed integrated framework and providing conclusions of the research. The following groups of themes identified in Chapter 4 are: i) compliance and regulations, ii) risk, strategy, responsibility and security control and iii) knowledge, communication, training and productivity.

After analysing the data in Chapter 4, a major risk is identified at the lower level of employees and in the Administration department. Most of these employees do not know about compliance and are unaware of compliance and its procedures. Communication, training and knowledge are identified as possibly being the root cause for this, and in order to mitigate risk, the organisation could introduce quality organisational culture practices, which are further discussed in the chapter. Headlines findings, which are linked from the themes, framework constructs and factors are depicted in Table 4.2 and discussed in more detail in this chapter. This chapter ends with presenting a proposed Integrated Framework for Information Security Compliance and a final conclusion of the research.

**Theme 1: Compliance and Regulations**

**Headline Finding 1: Coercive isomorphism by means of regulatory pressure has a positive influence on information security governance (Table 4.2).**

According to Johnston (2013:36), “Institutional isomorphism is the process whereby organisations become similar to each other. The process leads organisations to modify their direction and behaviour to become compatible to their environmental characteristics.”.

Coercive isomorphism is when “…formal and informal pressures are exerted on organisations to follow and adopt certain institutionalized rules and practices from the society within the organisation functions.” (Hu *et al*., 2007:157). These coercive pressures appear when powerful institutions force less powerful institutions to

comply with rules and behaviour, in order to receive benefits and legitimacy. The powerful institutions are often in the form of government, regulatory bodies and accreditation organisations. The benefits that less powerful institutions receive come for example, in the form of better resources and accreditation. The consequences of not complying with these coercive pressures are actions such as sanctions, penalties and fines, which could ultimately result in expulsion (Johnston, 2013).

It is evident in the findings (Table 4.2: Finding 1 & 21) that regulatory pressure from the FSB and legislature positively influences governance. This can be derived from security controls that have been put into place and are required by such laws and regulations (Table 4.2: Security control). Most of the employees of the organisation under discussion, arer aware that the regulator influences information security in the organisation, and becomes the critical reason for compliance (Table 4.2: Finding 1 & 21). It assists by introducing policies and guidelines for the organisation to implement, thus, reducing risk and improving governance. Employees across all departments are found to be the most aware of the POPI and FICA acts (Finding 33). In contrast, other legislature and policies are known to employees in the legal and IT departments (Table 4.2: Finding 33). Governance is found to stimulate best practice within business processes and therefore, improving information security (Table 4.2: Governance). This is supported by Hu *et al*. (2007) reporting that external forces influence diffusion in the organisation and that the internal forces in turn, influences creation from within. They further find that external sources also have an influence in shaping information security policies.

**Headline Finding 2: Normative isomorphism by means of internal and external stakeholder pressure has a positive influence on information security governance (Table 4.2).**

Normative isomorphism is when the "..professionalization of organisation actors occurs. They have similar training and education and occupy similar positions over a range of organisations." (Hu *et al*., 2007:157). The normative pressure exerted by internal and external stakeholders can be confirmed as being positive. It influences employees to be more vigilant and aware that they need to comply for greater reasons, other than themselves. When employees follow best practice norms and

guidelines in organisations, one of the reasons for doing this is fulfilling their job responsibilities, and to make a good impression on colleagues, management and clients. This has a favourable influence on information security compliance. This is supported by Johnston (2013) saying the influence of this normative pressure has a substantial influence on whether organisation are legitimate or not. The characteristics of employees within organisations can have an influence on getting organisations to move closer to conformity.

**Headline Finding 3: Mimetic isomorphism by means of industry pressure has little to no influence on information security governance (Table 4.2).**
Mimetic isomorphism is when the "…organisation mimics or imitates other organisations. This aids in reducing risks especially when the organisation faces challenges which are similar to other organisations." (Hu *et al.*, 2007:157).

It is found that pressure from industry is insignificant and employees do not believe it has much influence on whether they comply or not. There are a minimum number of employees who believe it does have some influence, but this is insignificant (Table 4.1: Finding 8, 9 & 10). Other organisations in the financial services industry do not provide enough pressure to make any difference (Finding 8, 9 & 10). Organisations therefore follow their own governance practices unique to the organisation itself.

**Theme 2: Risk, Strategy, Responsibility and Security control**

**Headline Finding 4: Information security governance by means of risk management, strategy formulation, responsibility and security control has a positive influence on compliance with information security policies and regulations (Table 4.2).**
According to von Solms (2006:444), "Information security governance consists of the management of commitment and leadership, the organisational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms which all works together to ensure integrity , confidentiality and availability of the organisations electronic assets.". Hu *et al*. (2007) examine employees based on the rational choice theory, where they found that the perception of the benefit has the major influence on employees intended

behaviour. As a result of this, their research concludes that punishment on its own is ineffective to reduce the number of security breaches contained in security policies. The findings suggest that the consequences of not complying are not clear enough for employees to fully understand it. Responsibility of information security compliance should be used to motivate every employee in the organisation, to comply and not only relying on IT, as some employees have suggested.

Vance *et al.* (2012) argue that informal sanctions have a stronger effect than formal sanctions. Their findings also suggest that the impact of morals and benefits can be used as predictors of employee violations. This is consistent with the findings of the case study which suggests that employees do not have any motivation to comply with information security policies and laws (Table 4.1: Finding 25, 27, 29, 33, 35 & 38). A significant number of employees are unaware of the risk of non-compliance. This could be a potential area for improvement in strategic formulation discussions by means of continuous awareness programmes (Table 4.1: Finding 25, 27, 29, 33 & 41). When an employee is aware of their responsibility towards the security of an organisation, it could potentially assist in improving imformation security compliance.

The research confirms that information security governance positively influences information security compliance (Table 4.2: Governance). This is consistent with the views of employees in the organisation. They are of the opinion it is management that needs to enforce governance principles and policies (Table 4.1: Finding 22). While some employees think governance impedes their productivity, most of the employees believed it is a necessity to do business in the financial services industry to protect the organisation and clients (Table 4.1: Finding 36). Security control is acceptable in the organisation and most employees are not able to access information that is not meant for them, which increases compliance (Table 4.1: Finding 32). The clients, FSB and legislature ultimately influence good information security governance practices (Table 4.2: Governance).

**Theme 3: Knowledge, Communication, Training and Productivity**

**Headline Finding 5: Information security culture by means of increased knowledge, better communication, more training and improved productivity**

**has a positive influence on compliance with information security policies and regulations (Table 4.2).**

The research finds that employee behaviour has a significant influence on information security compliance. This is consistent with the finding of Parsons *et al.* (2014) who examine the relationship between an employee's knowledge of policies and procedures and the behaviour, whilst making use of their company computer. Their findings suggest that employee knowledge of policies and procedures have a significant influence on attitude reported behaviour. When employees are aware of the threats and dangers the organisation faces with regards to security threats, they are able to prevent such events from happening in a more effective manner (Parsons *et al.*, 2014). It is found that when employees are left out of the communication loop it leaves significant weak points for security threats to occur. It is found that training and awareness are given to employees during an induction programme, when they start working, but never again afterwards.

According to Cheng *et al.* (2013), a large number of security incidents occur as a result of employees who deter from existing security policies. Employees state if they are regularly trained and updated on new threats and policies, it would significantly improve information security compliance (Table 4.1: Finding 49). The findings suggest that employees forgot or simply do not know how to properly manage the organisations information so even if employees would want to protect the organisations information, they simply do not know how and have not been involved in the organisational learning process (Table 4.1: Finding 29, 30, 36, 37, 41, 46 & 49) The potential impact of mishandling information could be damaging to the organisation.

Guo (2013) states that employee security related behaviour can either, create threats, or prevent them in an organisation. An examples of this includes the way which employees handle their passwords or manage the organisations data. It is found that employees are not aware of the role they play in protecting information in their organisation (Table 4.1: Finding 22, 27, 29 & 35). Most employees believe it is the sole responsibility of the IT department (Table 4.1: Finding 34 & 35). If the

mindset and beliefs of employees are given more attention, it has the potential of significantly improving information security compliance (Guo, 2013).

Often security policies are items which reflect static documents, only to be of value at the time of creation, unless it is continuously monitored and improved, its goals will not be achieved (Flores *et al*., 2014). Organisational agency theory comes into practice and has an influence on governance practices. This is shown by the lack of organisational culture, emphasising the agent instead of the principle. Employees need to take more responsibility in implementing governance policies (Table 4.1: 22, 23, 25, 26, 27, 29, 30, 33, 34 & 35). Examining information security compliance in the case organisation, the integration of regulations, security control, knowledge, training, risks, strategies and responsibilities of employees, form the framework for the organisation to be compliant (Table 4.2). These factors have been identified and discussed as themes, and developed taking into consideration, the proposed theories as a lens to the data, as well as the framework constructs as proposed.

### 5.2 The proposed framework

The proposed framework, presented in Figure 5.1, draws from theories and frameworks such Neo-institutional theory (Table 4.2), the framework for the governance of information security by von Solms (2004) and the organisational culture model by Denison (Denison *et al*., 2004).

The research findings, then lead to determine which factors, and how significantly these influence information security compliance, within the organisation (Table 4.2). The research aims to support these findings by concurring with substantiated literature. Finally, a proposed framework is presented matching to the findings.

The framework is specific to the organisation used in the case study and can be applied for better understanding of the factors influencing information security compliance. This would enable managers to strategise and implement improved policies and process to improve information security compliance. The framework depicted in Figure 5.1, builds onto the initial conceptual framework developed in Figure 2.4.

The proposed framework integrates parts of the neo Neo-institutional theory which includes coercive (Regulatory) and normative (Stakeholder) pressures, which are significant in influencing the organisation (Table 4.2). Further, the framework for the governance of information security by von Solms (2004) is used which found factors such as risks, strategy, vision, mission, policy, management to have the most influence in the organisation (Table 4.2: Governance) and finally, Denison's (1990) organisational culture model. To include the factors which were lacking the most in the organisation is identified from the findings (Table 4.2: Culture). All regulations and legislature which affects the organisation are included. Further, the order to create continuous awareness in the organisation which include Sarbanes Oxley, King code, FICA, Graham Leach Bibley, Common law, ISO, ECT act, FAIS, Banks Act, POPI act, and Basel. This framework integrated organisational culture factors from Denison's organisational culture model. These factors include consistency which is underpinned by Strategic Direction and Intent, Goals and Objectives and Vision, involvement underpinned by Empowerment, Team Orientation and Capability Development, adaptability underpinned by Creating Change, Customer Focus and Organisational Learning and mission underpinned by Core Values, Agreement, Coordination/Integration (Table 4.2: Culture). The framework changed to an iterative design compared to that in the conceptual framework depicted in Figure 2.4, which is found to be needed in the organisation to continuously keep controlling, monitoring, improving, and auditing compliance objectives to increase information security compliance. The arrows represent where the process originates, carried through and ends.

The framework is implemented in the organisation in an attempt to increase information security compliance in the departments which are lacking such as, Administration. As a result of the researcher being employed at the case organisation, the researcher approached the organisation to adopt the iterative approach and pilot the framework as shown in Figure 5.1, by continuously monitoring and controlling of processes, as well as giving ongoing training to employees and keeping all of them up to date on the latest laws, regulations and policies.

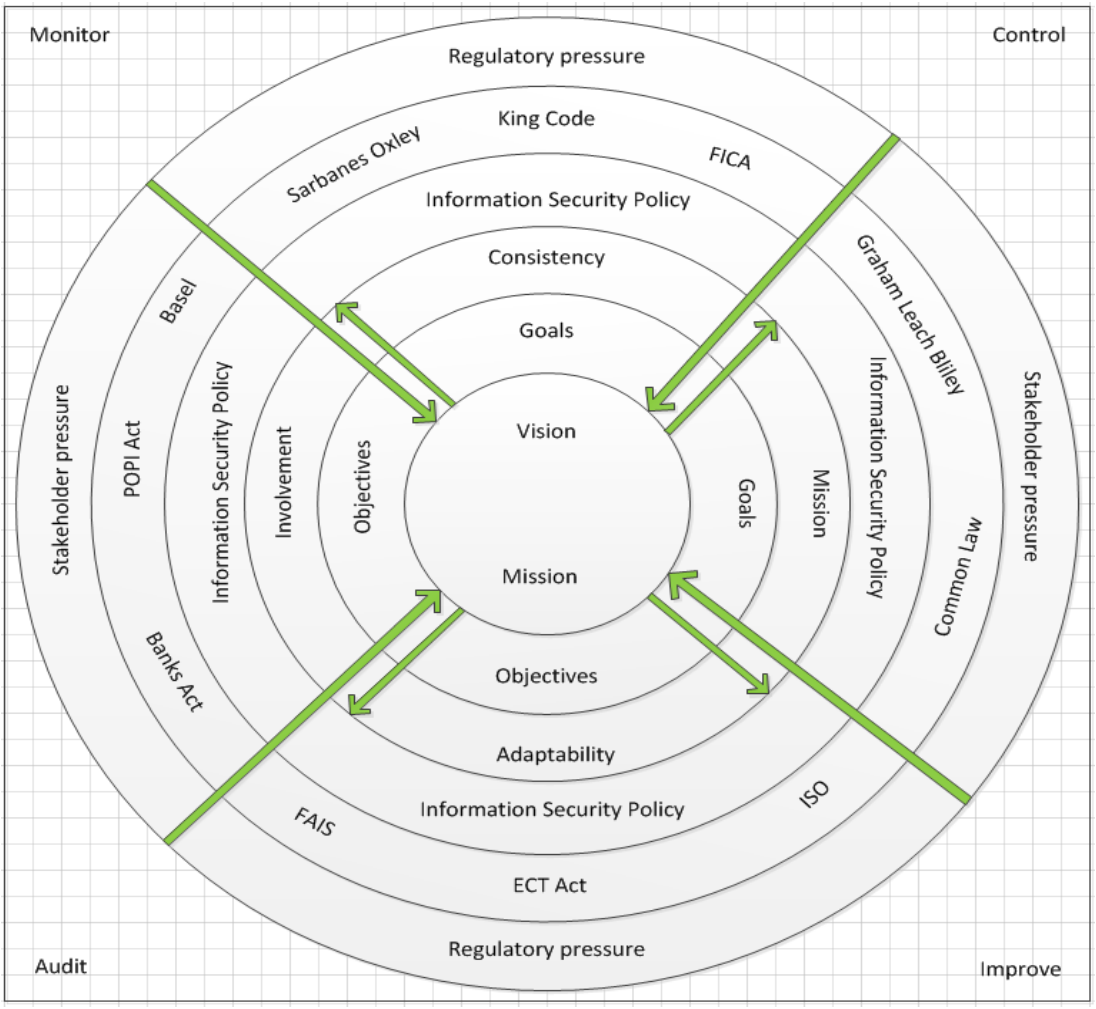


**Figure 5.1: Proposed Integrated Framework for Information Security Compliance**

## 5.3 Conclusions

According to the aims of the research, the researcher determines which factors, and how the factors influence compliance to information security policies and compliance. The goal remains, to design an integrated framework to assist in counteracting these findings where weaknesses are found. The researcher bases the findings on the Neo-institutional theory, Agency Theory, Rational choice theory, a framework for the governance of information security by von Solms and Denison's organisational culture model.

The research finds factors which a case organisation are confronted with, in order to ascertain if thery comply with laws regulations and information security policies to include the regulator, stakeholders, risks, strategy, vision, mission, policy, management and organisational culture. These factors are considered, how much influence each has in the organisation. Organisational security culture is found to be the least implemented in the organisation. In addition, consistency, involvement, adaptability and mission objectives are lacking which also poses a risk to the organisation. The proposed framework can assist to manage the impact, and influence organisational culture may have on the organisation. This can be integrated into the necessary levels in the process, to assist increasing information security compliance objectives.

The findings identify risks and strength areas to influence compliance through thematic analysis and key themes that are linked to these findings. The findings are then linked to findings which are consistent from literature. Using a financial services organisation as the case study for this research, interviews are conducted among employees at all levels of the organisation.

The FSB and legislature are found to have a strong coercive isomorphism influence on governance in the organisation. The pressure is consistent within the context of Neo institutional theory. These pressures include coercive pressures found such as FICA and POPI which showed to be significant in influence. This coercive pressure provides the baseline for external compliance requirements. The organisation is audited and frequently visited by the FSB to audit organisations conforming to regulations, thus motivating managers to act in accordance and implement positive actions in order to reach these compliance requirements this is confirmed by Johnston (2013).

The research finds that normative isomorphism which stemms from external and internal stakeholders, has an influence on information security compliance. Coercive isomorphism from regulators is found to be the most significant and has positive influence on information security compliance. Internal and external stakeholders influence processes for better monitoring and protection. It is evident that the client's

concern for their financial and personal information to be as secured as possible influence the way the organisation carries out their information processes. It plays a pivotal role in securing the organisation's network from hackers. The normative isomorphism can be confirmed as positive, as it influences positive information security strategies and goals for the organisation.

The least significant isomorphism is mimetic. This proves to have little influence in the way the organisation operates. It is found that the organisation rarely mimics what other organisations in the industry do. They pride themselves on being different and thus follow their own information security initiatives. The organisation deals with information security issues as being unique to their own organisation. The researcher was not able to delve to deep into this aspect with employees during interviews, but after analysis, came to the conclusion that the organisation is not significantly influenced by industry standards and pressure.

The research finds that information security governance has a positive influence on information security compliance. This is seen through policies and processes that have been put in place as security controls and measures. These findings are consistent with literature from Qassimi and Rusu (2015). Strategies and risk management influence the way the organisation plans for information security while management and legislature motivate the organisation to comply or face penalties. The influence is positive as it urges the organisation to comply to meet business requirements.

Information security culture plays a vital role in information security compliance. Employee behavior and attitude positively influence information security compliance. This is because employees who are more aware and trained behave in a compliant way. They believe that there is some kind of consequence if they do not. Lower level employees are found to be completely unaware of the compliance objections of the organisation poses the biggest threat. Communication and involvement from senior level through to lower level appears to be lacking. The Administration department shows the biggest threat to compliance as the department is not trained and communicates not effectively. When employees knowingly, protect the organisations

information, it assists to reach compliance objectives. Communication and organisational learning is found to be the key contributors to helping the organisation improve information security compliance.

### 5.4 Summary

Compliance and regulations themes by means of regulator pressure and stakeholder pressure in the organisation, prove to have a positive influence, while industry pressure has little to no influence on information security compliance in the organisation. Risk, strategy, responsibility and security control theme by means of information security governance proves to have a positive influence and when cultivated by knowledge, communication, training and productivity theme by means of good organisational culture increases information security compliance.

The following chapter (6) provides recommendations, reflection and contributions of the research.

# 6. Recommendations, reflection and contributions

Chapter 6 is structured as follows: i) recommendations are proposed followed by a reflection on the research.The contributions are described as i) contribution to IT, ii) law and compliance and iii) organisational culture. The chapter ends by highlighting the possible contribution made as a result of the research

## 6.1 Recommendations

The findings of this research opens up a valuable mechanism for organisations in the financial services industry, to strategise and prioritise compliance goals. Having a better understanding of the causes and how these influence each other, organisations will be able to implement processes that drive information security compliance. During the development of this research, a number of potential areas for future research became evident. Furthermore, the case study approach with the accompanying small data set obtained, the recommendations for future research is to expand the scope of the research. In addition, research into institutionalised pressures which affect the financial services industry, is another recommended future research area.

The research findings indicate that the regulator and stakeholder pressure to provide a significant positive influence on the organisation, while industry pressure has an insignificant influence on information security in the organisation. Information security culture cultivates governance and the two, when working together, increases information security compliance. By aligning organisational culture and governance goals, it may be more rewarding to the organisation in obtaining greater compliance especially, from employees.

The organisation needs to involve employees across all departments in compliance goals and an improved communication mechanisms required. The Administration department and lower level employees are the least knowledgeable about compliance and thus, poses the biggest risk to the organisation. Furthermore, the organisation should not only focus all their energy on senior level employees, but rather focus on carrying information security knowledge through from senior level all the way down to lower level employees. By integrating organisational culture into the

organisations processes, would decrease organisation risk where employees are not involved, trained and communicated to, effectively.

### 6.2 Reflection

As stated by the limitations of this research (Section 6.7) , the research follows a case study approach and is limited to a South African regulatory body and legislature. A challenge experienced during interviews relates to the integrity of some participants answering questions which are deemed sensitive. This is noted, and while participants answers to the best of their knowledge, some hostility is apparent from some senior and middle level employees. In order to gain wider insight into other organisations, it would have meant expanding the scope to include more organisations in the financial services industry. This journey where trust is essential, and achieving more easily managed interview communication sessions, is paramount to the success of obtaining valuable input from most participants.

The research findings from only one organisation is encouraging to plot the way for potential future research that can be explored on this topic in different organisations and even across different industries around the world. For this, the scope of such research needs to be expanded. However, the results of this research cannot be generalised about the Financial Services Industry. A number of factors are identified and is unique to this case organisation. Employees answered to the best of their knowledge, however, it is noted that responses may have been different with a different unit of analysis. The research results are as accurate as the answers received from the interviewees, and all based on their honesty. Further studies could also examine organisational and human factors to determine the effect this may have on information security compliance.

### 6.3 Contribution of Research

The literature review in Chapter 2 demonstrates there is not much information available that seamlessly unites the fields of information security, legal compliance and organisational culture. The lack of cohesion amongst these fields is problematic. At the core, the literature review reveals how the disciplinary boundaries are

solidified to the point where it is unproductive, resulting in organisations and consumers to have their security put at risk. There are few interdisciplinary studies how organisational culture intersects with issues such as, information security and technology, even much less on compliance. Therefore, this study contributes to the field in several important ways:

Firstly, the framework is implemented in the organisation and able to assist to increase information security compliance in the departments which are lacking for example, the Administration department. The organisation has adopted the iterative approach as depicted in Figure 5.1, where it ois possible to continuously monitor and control processes as well as providing ongoing training for employees. This is aimed at keeping all employees up to date on the latest laws, regulations and policies applicable to them.

### 6.4 Contribution to Information Technology

In keeping with the methodological contribution outlined above, the research enriches the field of information technology by providing information about law and compliance, that is accessible and actionable for information technology professionals. It integrates information about organisational culture with an eye on the unique and specific context, of information security compliance. The major contribution is enriching the field with a design, upholding interdisciplinary and sensibility to both, acknowledging the unique context of information security technology, and incorporating useful information from other fields. This, in order for information security departments to operate to their best possible standards.

### 6.5 Contribution to Law and Compliance

It is evident from the literature that the Law fraternity is not keeping pace with technology. The law fraternity tends to move at a gradual pace, whereas, technology moves at a much faster pace, akin to innovation. However, technology is still bound by legal regulations and therefore, the two fields are often popularly perceived as being at odds with one another. The field of Law tends to view technology as a runaway and reckless phenomenon, while technology tends to view Law as uselessly, slow and stodgy. Within this context, the research makes a major

contribution to the fields of Law and legal compliance, because it draws upon specific and actionable methods. These can then be used to improve the context of information technology as far as legal compliance is concerned. The thesis intends to bridge the disciplinary gap between Law and technology practice, such that the research provides a contribution in that it is informed by legal research, but intended for practical use.

### 6.6 Contribution to Organisational Culture

In terms of the contribution of this thesis it makes to the fields of organisational management and organisational culture, the anticipated contributions are manyfold. Firstly, the results present an opportunity to test some of the claims made by studies of organisational culture, and further, to test these within the relatively untried and new context of information technology and information security. Secondly, the resulst assumes as a given, that intangible assets, such as data and reputation, are just as vital to an organisation as buildings and equipment. Thirdly, the resulst, could engage with claims regarding organisational culture within a context of constraints: technological constraints, legal constraints, logistical constraints, organisational ones, and inter-organisational ones. Therefore, this research of organisational interventions will make a major contribution to interdisciplinary and inter-and intra-departmental organisational culture.

### 6.7 Limitations of Research

This research is not without limitations. The research is a case study based on a Financial Services Organisation in Cape Town, South Africa and thus, limited to the South African legislature and regulatory bodies. The research obtains findings from only one organisation and potential future research could be to explore this topic in different organisations, and across different industries around the world. The scope of the research limited the research to one organisation. The research does not generalise results about the Financial Services Industry. Although a number of factors are identified, this could be unique to this organisation. Interviews are conducted with 20 employees from the organisation, ranging from senior level to lower levels. Employees answers to the best of their knowledge, however, it is noted

that respondents could have been different with a different unit of analysis. However, the research is as accurate as the answers received from interviewees, based on their honesty. Further studies could also examine the organisational factors and human factors to determine the effect it might have on information security compliance.

The research identified factors affecting information security compliance to information security policies and regulations in a financial services organisation. These factors include the regulator, internal and external stakeholders, industry standards, information security governance and organisational culture. The research determines that the biggest risk to information security compliance objectives is in the lower level jobs and in the Administration department. Information security governance has a significant influence on compliance objectives. Sound organisational culture plays a vital role in increasing information security compliance, as this is done by cultivating things such as knowledge, communication and training.

**References**

Baxter, P., & Jack, S. 2008. Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report,* 13(4):544-559.

Bermejo, P.H. de S., Tonelli, A.O., Zambalde, A.L., Santos, P.A dos. & Zuppo, L. 2014. Evaluating IT governance practices and business and IT outcomes : A quantitative exploratory study in Brazilian companies. *Procedia Technology*, 16():849–857. http://www.sciencedirect.com/science/article/pii/S221201731400262X. [April 10, 2015].

Bernroider, E.W.N. & Ivanov, M. 2011. IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, 29(3):325–336. http://linkinghub.elsevier.com/retrieve/pii/S0263786310000529. [March 26, 2014].

BonJour, L. 2010. *Epistemology: Classic problems and contemporary responses.* Lanham, Md: Rowman & Littlefield Publishers.

Brannick, T., & Coghlan, D. 2007. In defence of being "native": The case for insider academic research. *Organisational research meth*ods, 10(1):59-74.

Bryman, A. & Bell, E. 2011. *Business research methods* (3rd ed). Oxford: Oxford University press.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. 2013. Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39():447–459. http://linkinghub.elsevier.com/retrieve/pii/S0167404813001387. [March 26, 2014].

Ciarlone, L. 2006. Eliminating the Fear Factor: Creating a Culture of Compliance. The Gilbane Group. http://www.omtool.com/wp-content/uploads/documents/eliminatingFearFactorWhitepaper.pdf. [March 26, 2014].

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. & Baskerville, R. 2013. Future directions for behavioral information security research. *Computers & Security,* 32():90–101. http://linkinghub.elsevier.com/retrieve/pii/S0167404812001460. [March 26, 2014].

D'Arcy, J., Hovav, A. & Galletta, D. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, ():79-98.

Da Veiga, A. & Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207. http://linkinghub.elsevier.com/retrieve/pii/S0167404809000923. [March 26, 2014].

Damianides, M. 2004. How does SOX change IT? *Journal of Corporate Accounting & Finance*, 15(6):35-41.

David, B. & Resnik J.D. 2011. What is Ethics in Research & Why is it Important? *National Institute of Environmental Health Sciences.May 2011:* 1-10.

Denison, D.R., Haanland, S. & Goelzer, P. 2004. Corporate Culture and Organisational Effectiveness. *Organisational Dynamics,* 33(1):98–109. http://linkinghub.elsevier.com/retrieve/pii/S0090261603000731. [ March 26, 2014]

Dimaggio, P.J. & Powell, W.W. 1983. The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields. *American Sociological Review*, 48(2):147-160.

Dimitriadis, C. 2011. Information Security from a Business Perspective. *ISACA Journal* 1(1):43-48.

Donaldson, L. & Davis, J.H. 1991. Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns. *Australian Journal of Management*, 16():49–64.

Eisenhardt, K.M. 1989. Agency Theory: An Assessment and Review. Academy of Management Review, 14():57–74.

Fayezi, S., O'Loughlin, A. & Zutshi, A. 2012. Agency theory and supply chain management: a structured literature review. *Supply Chain Management: An International Journal,* 17(5):556–570.

Financial Advisory and Intermediary Act. 2002. https://www.fsb.co.za/feedback/Documents/Financial%20Advisory%20and%20Intermediary%20Services%20(FAIS)%20Act.pdf. [April 10, 2015].

Fisher, C., Buglear, J., Lowry, D., Mutch, A. & Tansley, C. 2010. *Research and Writing a Dissertation.* Harlow: Prentice Hall.

Flores, R.W., Antonsen, E. & Ekstedt, M. 2014. Information security knowledge sharing in organisations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43():90–110. http://linkinghub.elsevier.com/retrieve/pii/S0167404814000339. [April 10, 2015].

Ford, R. & Wiedemann, J. 2010. *The Internet case study book*. Köln: Taschen.

Fredriksson, M., Pallas, J. & Wehmeier, S. 2013. Public relations and neo-institutional theory*. Public Relations Inquiry*, 2(2):83–203.

Freeman, E.H. 2007. Regulatory Compliance and the Chief Compliance Officer. *Information Systems Security,* 16(6):357–361. http://www.tandfonline.com/doi/abs/10.1080/10658980701805050. [March 5, 2014].

Gerber, M. & von Solms, R. 2005. Management of risk in the information age. *Computers & Security*, 24(1):16–30. http://linkinghub.elsevier.com/retrieve/pii/S0167404804002780. [July 29, 2014].

Gerber, M. & von Solms, R. 2008. Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27(5-6):124–135. http://linkinghub.elsevier.com/retrieve/pii/S0167404808000461. [May 19, 2014].

Gerring, J. 2006. *Case study research: principles and practices*. Cambridge:Cambridge University Press.

Gladwell, M. 2013. *David and Goliath: Underdogs, Misfits, and the Art of Battling Giants.* New York: Little, Brown.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Sohail, T. 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5):503–530. http://linkinghub.elsevier.com/retrieve/pii/S0278425406000652. [March 5, 2014].

Gotlieb, J.B. & Swan, J.E. 1990. *An Application of the Elaboration Likelihood Model*.

Gray, J.T. 2008. *Neoinstitutional Theory* : SAGE Knowledge. In International Encyclopedia of Organisation Studies. London: SAGE:957–959.

Greenwood, R. & Hinings, C.R. 1996. Understanding radical organisational change: Bringing together the old and the new institutionalism. *Academy of Management Review*, 21(4):1022–1054.

Guo, K.H. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32(1):242–251. http://linkinghub.elsevier.com/retrieve/pii/S0167404812001666. [March 26, 2014].

Halliday, J. & von Solms, R. 1997. *Effective Information Security Policies*, In von Solms, R. (Ed), Information Technology on the Move,:12 – 20, Port Elizabeth: Port Elizabeth Technikon.

Hechter, M. & Kanazawa, S. 1997. Sociological Rational Choice Theory*. Annual Review of Sociology,* 23():191–214.

Herath, T. & Rao, H.R. 2009a. Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165. http://linkinghub.elsevier.com/retrieve/pii/S0167923609000530. [January 24, 2014].

Herath, T. & Rao, H.R. 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations*. European Journal of Information Systems*, 18(2):106–125. http://www.palgrave-journals.com/doifinder/10.1057/ejis.2009.6. [January 25, 2014].

Hinson, G. 2003. *Human factors in information security*. http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf [March 26, 2014].

Hu, Q., Hart, P. & Cooke, D. 2007. The role of external and internal influences on information systems security – a neo-institutional perspective*. The Journal of Strategic Information Systems*, 16(2):153–172. http://linkinghub.elsevier.com/retrieve/pii/S0963868707000212. [March 26, 2014].

Hussein, A. & Al-Tamimi, H. 2008. Implementing Basel II: an investigation of the UAE banks. Basel II preparations. *Journal of Financial Regulation and Compliance*, 16(2):173–187. http://www.emeraldinsight.com/10.1108/13581980810869814. [March 5, 2014].

Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.

*Computers & Security*, 31(1):83–95. http://linkinghub.elsevier.com/retrieve/pii/S0167404811001337. [February 20, 2014].

Ifinedo, P. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), pp.69–79. http://linkinghub.elsevier.com/retrieve/pii/S0378720613000980. [March 23, 2014].

IT Governance Institute. 2006. *Information Security Governance: Guidance for Boards of Directors and Executive Management Guidance for Boards of Directors and Executive Management.* Rolling Meadows, Illinois: ISACA.

IT Governance Institute. 2007. *Information Security Governance: Guidance for Information Security Managers.* Rolling Meadows, Illinois: ISACA.

Johnston, M. 2013. *Mimetic, Coercive and Normative Influences and the Decision of National Sport Organisations to Bid for World Championship Events*.http://aut.researchgateway.ac.nz/bitstream/handle/10292/7182/JohnstonM.pdf?sequence=3. [April 10, 2015].

Jurkus, A.F., Park, J.C. & Woodard, L.S. 2011. Women in top management and agency costs. *Journal of Business Research*, 64(2):180–186.

Kerr, D.S. & Murthy, U.S. 2013. The importance of the CobiT framework IT processes for effective internal control over financial reporting in organisations: An international survey. *Information and Management*, 50(7):590–597. http://dx.doi.org/10.1016/j.im.2013.07.012. [April 10, 2015].

Kolkowska, E. & Dhillon, G. 2013. Organisational power and information security rule compliance. *Computers & Security*, 33():3–11. http://linkinghub.elsevier.com/retrieve/pii/S0167404812001010. [April 10, 2015].

Luthy, D. & Forcht, K. 2006. Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security*, 14(2):155–166. http://www.emeraldinsight.com/10.1108/09685220610655898. [March 5, 2014].

Maphakela, R. & Pottas, D. 2006. Towards Regulatory Compliance: A Model for the South African Financial Sector. *ISSA Conference Proceeding.*

Marnewick, C. & Labuschagne, L. 2011. An investigation into the governance of information technology projects in South Africa. *International Journal of Project Management*, 29(6):661-670.

Mitnick, K.D. & Simon, W.L. 2003. The Art of Deception: Controlling the Human Element in Security. *BMJ: British Medical Journal*, ():368. http://www.bmj.com/content/347/bmj.f5889. [April 10, 2015].

Myers, M.D. 2010. *Qualitative research in business and management*. London: Sage Publications.

Neuman, W. L. 2010. *Social Research Methods Qualitative and Quantitative Approaches*. 7th ed: Pearson.

Parliament of the Republic of South Africa. 2013. *South Africa Protection Personal information Act*, *2013*. Pretoria:National Gazette, No 37067, (10505):1–148. http://www.greengazette.co.za/notices/act-no-4-of-2013-protection-personal-information-act-2013_20131126-GGN-37067-00912. [April 10, 2015].

Parliament of the Republic of South Africa. 2002. *South Africa Electronic Communications and Transactions Act, 2012*. Pretoria: National Gazette. Available at http://www.gov.za/sites/www.gov.za/files/a25-02.pdf. [April 10, 2015].

Parliament of the Republic of South Africa. 2001. *The Financial Intelligence Centre Act, 2001*. Pretoria:National Gazette.

https://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/FIC%20Act%20Booklet%20202012.pdf. [April 10, 2015].

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42():165–176. http://linkinghub.elsevier.com/retrieve/pii/S016740481300179X. [April 10, 2015].

Petty, R. & Cacioppo, J. 1986. *The elaboration likelihood model of persuasion.* Advances in experimental social psychology. San Diego, CA: Academic Press, 19():123–162.

Pinder, P. 2006. *Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II).* Information Security Technical Report, 11(1):32–38. http://linkinghub.elsevier.com/retrieve/pii/S1363412705000786. [March 26, 2014].

Posthumus, S. & von Solms, R. 2004. *A framework for the governance of information security.* Computers & Security, 23(8):638–646. http://linkinghub.elsevier.com/retrieve/pii/S0167404804002639.[June 15, 2014].

PricewaterhouseCoopers. 2003. The Compliance Gap. *Journal of Investment Compliance*, 4(1):31-38.

Racz, N., Weippl, E. & Seufert, A. 2010. A process model for integrated IT governance, risk, and compliance management. *Databases and Information Systems. Proceedings of the Ninth International Baltic Conference, Baltic DB&IS 2010*. Riga: University of Latvia Press, ():155-170.

Qassimi, N.A. & Rusu, L. 2015. IT Governance in a Public Organisation in a Developing Country: A Case Study of a Governmental Organisation. *Procedia Computer Science,* 64():450–456. http://linkinghub.elsevier.com/retrieve/pii/S1877050915026769. [April 10, 2015].

Ruighaver, A.B., Maynard, S.B. & Chang, S. 2007. Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1):56–62. http://linkinghub.elsevier.com/retrieve/pii/S016740480600157X. [July 12, 2014].

Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research Methods for Business Students*. 5th edition. Harlow UK: Pearson Educational.

Saunders, M., Lewis, P. & Thornhill, A. 2016. *Research Methods for Business Students*. 7th edition. Harlow UK: Pearson Educational.

Shapiro, S.P. 2005. Agency theory. *Annual Review of Sociology*, 31():263–284.

Shropshire, J., Warkentin, M. & Sharma, S. 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*,():1–18. http://dx.doi.org/10.1016/j.cose.2015.01.002. [April 10, 2015].

Siponen, M., Mahmood, M.A & Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224. http://linkinghub.elsevier.com/retrieve/pii/S0378720613001237. [April 10, 2015].

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J. 2013. Variables influencing information security policy compliance. *Information Management & Computer Security*, 22(1):42–75. http://www.emeraldinsight.com/doi/abs/10.1108/IMCS-08-2012-0045. [March 10, 2014].

Thomson, K. & van Niekerk, J. 2012. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, 20(1):39–46. http://www.emeraldinsight.com/10.1108/09685221211219191. [March 26, 2014].

University of Twente. 2014. *Elaboration Likelihood Model*. http://www.utwente.nl/cw/theorieenoverzicht/Theory_clusters/Health_Communication/Elaboration_Likelihood_Model/ . [April 10, 2015].

Van Niekerk, J.F. & Von Solms, R. 2010. Information security culture: A management perspective. *Computers & Security*, 29(4):476–486. http://linkinghub.elsevier.com/retrieve/pii/S0167404809001126. [March 26, 2014].

Vance, A., Siponen, M. & Pahnila, S. 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3-4):190–198. http://linkinghub.elsevier.com/retrieve/pii/S0378720612000328. [March 26, 2014].

Veiga, A. & Martins, N. 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49():162–176. http://dx.doi.org/10.1016/j.cose.2014.12.006. [April 10, 2015].

von Solms, B. 2001. Information Security – A Multidimensional Discipline. *Computers and Security*. Vol 20, (6):504-508. http://www.sciencedirect.com/science/article/pii/S0167404801006083. [March 26, 2014].

von Solms, B. 2005. Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2):99–104. http://linkinghub.elsevier.com/retrieve/pii/S0167404805000210. [March 26, 2014].

von Solms, B. 2006. Information Security – The Fourth Wave. *Computers & Security*, 25(3):165–168. http://linkinghub.elsevier.com/retrieve/pii/S016740480600054X [March 26, 2014].

von Solms, S.H. 2005. Information Security Governance – Compliance management vs operational management. *Computers & Security*, 24(6):443–447. http://linkinghub.elsevier.com/retrieve/pii/S0167404805001057. [April 03, 2014].

von Solms, R. & von Solms, B. 2004. From policies to culture. *Computers & Security*, 23(4):275–279. http://linkinghub.elsevier.com/retrieve/pii/S0167404804000331. [March 24, 2014].

von Solms, R. & von Solms, S.H. 2006. Information security governance: Due care. *Computers & Security*, 25(7):494–497.

Vroom, C. & von Solms, R. 2004. Towards information security behavioural compliance. *Computers & Security*, 23(3):191–198. http://linkinghub.elsevier.com/retrieve/pii/S016740480400032X. [April 03, 2014].

Warden, S.C. 2007. E-Commerce adoption by SMMEs - How to optimise the prospects of success. Unpublished DTech (IT) thesis, Cape Peninsula University of Technology, Cape Town, South Africa.

Whiting, L.S. 2008. Semi-structured interviews: guidance for novice researchers. *Nursing Standard*, 22(23):35.

Wilson, J. 2014. *Essentials of business research. A guide to doing your research project.* Second edition:149 – 151.

Yin, R.K. 2013. *Case Study Research: Design and Methods.* California: Sage Publications.

Yin, R.K. 2003. *Case Study Research: Design and Methods*. California: Sage Publications.

Zagzebski, L.T. 2009. *On epistemology*. Belmont, CA: Wadsworth Cengage Learning.

Zhang, J. & Sarathy, R. 2009. Understanding Compliance with internet use Policy from the Perspective of Rational Choice Theory. *Decision Support Systems*, 9(4):635-645.

**Appendix 1 – Interview guide**

**RQ 1:** What factors do organisations face in order to comply with laws, regulations and information security policies?

***SRQ 1.1*** *What are the information security compliance approaches that financial services organisations deploy?*

IQ 1.1.1) Does the FSB and government ensure your organisation complies with regulations?

If yes, why?

If no, why not?

IQ 1.1.2) Do you have specific corporate compliance approaches/strategies?
If yes, what are they?

If no, why not?

IQ 1.1.3) In your opinion, how well are your information security policies enforced?

IQ 1.1.4) Does your organisation comply with the regulation because of industry standards?
If yes, why?

If no, why not?

***SRQ 1.2*** *What are the challenges, financial services organisations faces in order to comply with the regulatory body's laws and guidelines?*

IQ 1.2.1) According to you, what are the major factors considered in complying with the regulator?

IQ 1.2.2) What challenges are you experiencing when facing these factors to an attempt to comply?

IQ 1.2 3) How do you overcome the challenges you are facing?

**RQ 2: How does the information security culture influence compliance to information security policies and regulations?**

***SRQ 2.1 How does governance influence information security compliance?***

IQ 2.1.1) Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security?
If yes, why?

If no, why not?

IQ 2.1.2) How do regulations and policies influence your organisation's information security?

IQ 2.1.3) What role does management play in the implementation of information security compliance?

*SRQ 2.2 How does employee information security knowledge influence compliance?*

IQ 2.2.1) Are you regularly informed of any changes in compliance requirements?
If yes, why?

If no, why not?

IQ 2.2.2). Are you are aware of the risk of non-compliance?
If yes, why?

If no, why not?

IQ 2.2.3) What do you do when faced with information security problems?
If yes, why?

If no, why not?

IQ 2.2.4) Do you access information that is not meant for you?
If yes, why?

If no, why not?

IQ 2.2.5) Do you know of any rules or regulations that exist around information?
If yes, what?

If no, why not?

IQ 2.2.6) Who is responsible for the security of your organisations information?

***SRQ 2.3 How does information security compliance affect employee performance?***

IQ 2.3.1) Do you think observing, tracking and notification of security incidences are part of your daily work routine?
If yes, why?

If no, why not?

IQ 2.3.2) In your opinion does complying with policies and regulations hamper your productivity?
If yes, why?

If no, why not?

***SRQ 2.4*** *How do organisations manage the potential reputational damage that fragmented compliance approaches create?*

IQ 2.4.1) Do you think protection of information is part of the organisation's strategy?
If yes, why?

If no, why not?

IQ 2.4.2) Do you think the organisation evaluates past security experiences?
If yes, why?

If no, why not?

IQ 2.4.3) Does your organisation have a data backup and disaster recovery plan?
If yes, why?

If no, why not?

IQ 2.4.4) Are risk vulnerability checks constantly conducted in your organisation?
If yes, why?

If no, why not?

IQ 2.4.5) Is creating user awareness on security threats is part of education and training for the organisation?
If yes, why?

If no, why not?

## Appendix 2: Summary of interview responses

Summary of interview responses below.

| | | Interviewee 1 - Network Administrator, Middle, IT | Interviewee 2 - Business Analyst, Middle, IT | Interviewee 3 - Payroll Manager, Senior, HR | Interviewee 4- Marketing administrator, Middle, Marketing | Interviewee 5- Finance clerk, Middle, Finance | Interviewee 6 - Financial advisor, Middle, Sales |
|---|---|---|---|---|---|---|---|
| IQ 1.1.1) | Does the FSB and government ensure your organisation complies with regulations? | Yes, because they regulate what organisations should comply with | Yes, there is any information regulations we need to comply with | Yes I think so | I don't know, because I'm not involved in that part of the business | Yes all financial organisations must comply to them | Yes, in order to ensure that we behave in a fit and proper manner and treat customers fairly |
| IQ 1.1.2) | Do you have specific corporate compliance approaches/strategies? | Yes, all document must be filled in honestly | I think FAIS and other compliance approaches. | Yes we do | I don't know | I don't know really, not involved in strategy making | Compliance checks |
| IQ 1.1.3) | In your opinion how well are your information security policies enforced? | Very well | I am not sure, but I can say that is well enforced. | I think they are enforced well | I think they are enforced very good | I would think quite well | Very well |
| IQ 1.1.4) | Does your organisation comply with regulation because of industry standards? | Yes, because they are forced to by the government | Yes, to avoid charges or penalties. They also help to put some structure in the business | I don't think so, we comply in order to protect our clients and to be able to operate in the industry | Im not sure what the specific reason for complying with the regulator is | No I think they comply so they don't land up in trouble | Yes, because of the risk involved with non compliance |
| IQ 1.2.1) | According to you what are the major factors considered in complying with the regulator? | That all information supplied are correct and truthfully filled in | I don't know | I think it would be to change certain processes in order to comply to new regulations | I don't know | Information that is complete | Behaving in a fit and proper manner, treating customers fairly & information security and confidentiality |
| IQ 1.2.2) | What challenges are you experiencing when facing these factors to an attempt to comply? | That investors don't truthfully fill in the required information | I don't know | Building new efficient processes | I don't know | Clients not completing their information properly | Clients misinterpreting the law |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 1.2 3) | How do you overcome the challenges you are facing? | We require proof of all information | I don't know | By being persistent to overcome these challenges | I don't know | Make sure you go over it with them until its correct | Stick to our companies policies and procedures and comply with the regulation |
| IQ 2.1.1) | Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security? | Yes, because stakeholders information is private and confidential and the law requires it to be kept that way. | Yes, for our customers to be comfortable with giving their information. | We comply because we have to in order to operate in the financial sector however our clients are our priority and we try to satisfy all their needs | I don't know | We comply in order to do business in the sector | Yes, we comply in order to protect our business and its clients |
| IQ 2.1.2) | How do regulations and policies influence your organisations information's security? | They have to keep a strict hold on all its information. | information security policies are vital to protect and secure our data | They ensure that we protect our information to their standards | They assist management with guidelines | They make sure its more secure | It barely influences our company because our company already follows strict policy and procedure on its own |
| IQ 2.1.3) | What role does management play in implementation of information security compliance? | They ensure that all information security gets complied with. | I am not in management so I do not know management strategies to ensure information security | They are there to implement and maintain | They are the implementers and enforcers | They are the ones who has to make sure we are complying with the regulator or governement | A major role as they ensure that it is enforced |
| IQ 2.2.1) | Are you regularly informed of any changes in compliance requirements ? | No, it does not form a major part of my job. | Yes, to adhere to regulations. We also make changes on our payroll system to comply | Yes most times | Yes if it pertains to me | Yes most times | Yes, in order for our company to comply with new/changes to regulation |
| IQ 2.2.2) | Are you are aware of the risk of non-compliance? | Yes, because I learned it through my career. | Yes, accountable officers will get penalties or fines | Penalties and fines | No I don't know I just know that its bad | Not fully aware just know that there will be consequences | Yes, so that we are aware of the implications |
| IQ 2.2.3) | What do you do when faced with information security problems? | I take the issue to my manager. | Send the query to compliance department | We tackle the issue and resolve accordingly, depends on the problem and the people involved | I call on my manager | Im not sure I never faced anything yet and I am not sure on the procedures to follow | Raise it with my HOD |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 2.2.4) | Do you access information that is not meant for you? | No, because it is not meant for me. | No, our systems security levels are tightened according to job org structure . | No I can only see information that's meant for me through access control | No im not allowed to | Not really I don't go looking for stuff that's not meant for me | No, each individual only has access rights to what they require access to |
| IQ 2.2.5) | Do you know of any rules or regulations that exist around information? | Yes, all information is private and confidential. | Yes, sharing of information (PPI) | Yes there are many such as POPI | No not really I just know that there are | Not really, I know there is just not sure what | Yes, how to store and save information |
| IQ 2.2.6) | Who is responsible for the security of your organizations information? | My manager and my team. | Compliance Officers. | IT | IT | Probably senior management | I.T |
| IQ 2.3.1) | Do you think observing, tracking and notification of security incidences are part of your daily work routine? | Yes, because I know it is part my work routine. | No, I am a BA in systems | Yes if something comes up I will notify IT | No I don't think so because I would know | No not that im aware of | No, I only raise it if it occurs |
| IQ 2.3.2) | In your opinion does complying with policies and regulations hamper your productivity? | No, because if you are going to do something then do it right. | Yes, I have to make sure that when reporting employee information it does not end up in the wrong hands, and this process of checking may take time. | No not really because it is part of my responsibiliti es | No I don't notice if it does | Yes because we have extra things to do but that's part of the job | Yes, it slows productivity but it is necessary |
| IQ 2.4.1) | Do you think protection of information is part of the organisation's strategy? | Yes, because they are forced to by the government. | Yes, to be a trusted organization to our employees | I think so yes because its important | Yes most probably because our information is important | No there are more important things | Yes, because our clients information is confidential |
| IQ 2.4.2) | Do you think the organisation evaluates past security experiences? | Yes, because they use this experience to better their security. | Yes, to get a feel of what to expect | Yes we learn from our mistakes | Yes I do think so so that they can fix errors of the past so that it don't happen again | Im not sure never heard of it yet | Yes, in order to improve |
| IQ 2.4.3) | Does your organisation have a data backup and disaster recovery plan? | Yes, because if the first sight explodes then the backup plan will allow them to continue doing business. | Yes, backup to ensure that we can roll back anytime. Disaster recovery for business continuity during disaster. | Yes we do in order to protect us from any fires and disasters | Yes we have an offsite | Yes I think so | Yes, to be safe and not lose everything in the event of a disaster |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 2.4.4) | Are risk vulnerability checks constantly conducted in your organisation? | Yes, because they need to ensure that risk is kept to a minimum. | I don't know. Risk and compliance office would know. | Im not sure about that | I don't know | Not that im aware of | Yes, to check if/ where there are any gaps in the system and improve on them |
| IQ 2.4.5) | Is creating user awareness on security threats is part of education and training for the organisation? | Yes, if everyone in the organization is aware of the risks then everyone can work together to mimise them. | Yes, to minimize the risk | I don't think its ongoing but we are made aware of anything major | I don't know | No its not Ive never received proper training on threats | Yes, so you are aware of the importance |

| | | Interviewee 7 - Secretary, Low, Admin | Interviewee 8 - Systems Analyst, Middle, IT | Interviewee 9 - Admin supervisor, Senior, Admin | Interviewee 10- Admin clerk, Middle, Admin | Interviewee 11- Financial Advisor, Middle, Sales | Interviewee 12 - Web designer, Middle, Marketing |
|---|---|---|---|---|---|---|---|
| IQ 1.1.1) | Does the FSB and government ensure your organisation complies with regulations? | I have no idea | Yes it does. Wê always ensure that our organization is 100% compliant to existing and new regulations | Yes as the organization has to comply with certain SA and UK laws | I think so yes | Yes, Financial industry is constantly regulated to ensure best practices. | Yes, they send out auditors to check if the company is complying with rules and regulations in relation to information security. |
| IQ 1.1.2) | Do you have specific corporate compliance approaches/strategies? | I don't know | Our governmental and external compliance strategy is managed through an external vendor | Yes , legal department and auditors | Im not sure | Yes | No, it differs from company to company depending on the business trade. |
| IQ 1.1.3) | In your opinion how well are your information security policies enforced? | I don't know | We have adequate cover as we have not had any breach in security as yet | Very well | I think it must be good we are a financial organisation | Very well, no information is disclosed unless consent has been given by the client | Not well enough, there are countless cases of credit card and identity fraud happening in today's day and age |
| IQ 1.1.4) | Does your organisation comply with regulation because of industry standards? | I don't know | Yes we do as we need to remain compliant | Yes but it has little influence on our operations | Im not sure Ive never came across it | Yes and based on Global standards that have not been implemented in SA yet | Yes they do, each level of security compliance is measured against industry standards, they can be fined if it doesn't measure up. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 1.2.1) | According to you what are the major factors considered in complying with the regulator? | I don't know | These are driven by cost, ease of implementation and ease of management | Loss of revenue | Im not sure I don't deal with the regulator | Financial advisory intermediary services act – money laundering | Information should be true and available upon request |
| IQ 1.2.2) | What challenges are you experiencing when facing these factors to an attempt to comply? | I don't know | Our current challenges are getting all our sites around Africa compliant and a cost effective rate | Accurate information that is readily available | I don't experiences any | Correct processes are in place so I do not find anything challenging | Consumers aren't always truthful with their information. |
| IQ 1.2 3) | How do you overcome the challenges you are facing? | I deal with them with assistance from colleagues | Because these are regulations we have to cost cut 'n other areas to make these effects realistic | We try to keep our data integrity to the highest standard | I take it up with my manager | Gathering information, finding out the source of funds etc. | You need to have guidelines in place in order to validate consumers' information. |
| IQ 2.1.1) | Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security? | I have no idea | Yes we do as we need to respect the organization stakeholders and their right to privacy | Yes | Im not sure but I think it would be to protect the client | Yes, to protect the consumer | Yes, if theres a loss of personal information the organization can be sued. |
| IQ 2.1.2) | How do regulations and policies influence your organisations information's security? | I don't know | We have strict regulations that is managed strictly through our IT department | Positive influence | They must make sure that everything complies | They increase information security in the business by hampering what employees can or cant do | Regulations and Policies are implemented by law. Your organisation's information security needs to abide by that law in order to do business legally. |
| IQ 2.1.3) | What role does management play in implementation of information security compliance? | I don't know | Management plays a small role as their main concern us running the operations of the business | Ensuring all regulations are complied and regularly auditing information | They implement security measures | Ensures that the correct processes are in order to comply with regulations. | Management needs to ensure that all information security guidelines abides with these of the Regulator |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 2.2.1) | Are you regularly informed of any changes in compliance requirements ? | sometimes, I guess it depends on what type of change it is and if im involved in it | Yes, we have regular forums where possible changes if any are discussed and decided on | Yes as this will briefed and we will also have to brief team members | No, im not sure why not | Yes, to ensure that correct processes are followed and applied according to regulations. | Yes, it's the organisation's responsibility to keep the employee up to date with any changes to compliance requirements. |
| IQ 2.2.2) | Are you are aware of the risk of non-compliance? | No, I don't know | Yes we are, those shortfall are available in our disaster recovery | Yes if we don't comply we face fines or if its serious then prosecution | No I don't know I was never informed | Yes | No, in some cases like now employees are oblivious to the risks of non-compliance |
| IQ 2.2.3) | What do you do when faced with information security problems? | Do whatever I need to do, inform management | We address the issue at hand and work on preventing any future occurrences | Get the necessary stakeholders involved to reolve the issue | I tell my manager | Escalate it | You analyse the issues and work out a plan of action to fix the issues. |
| IQ 2.2.4) | Do you access information that is not meant for you? | No | No, we have user roles configured for this reason | no | I don't have access | No, there is no access to information not needed | No, unless authorized to do so. |
| IQ 2.2.5) | Do you know of any rules or regulations that exist around information? | No, I don't know | No unfortunately not. | yes | You not allowed to use someones information without their permission | Yes | Copyright laws |
| IQ 2.2.6) | Who is responsible for the security of your organizations information? | IT | IT | IT | IT | IT | That would be the employees responsible for maintaining the information server such as IT |
| IQ 2.3.1) | Do you think observing, tracking and notification of security incidences are part of your daily work routine? | I don't know | It is not as its managed through our IT department | Yes I do to manage my team | No it was never part of it because nobody informed me to do it | Yes | Yes, you need to ensure that information is protected at all times |
| IQ 2.3.2) | In your opinion does complying with policies and regulations hamper your productivity? | I don't really know | It shouldn't as these tasks are there to improve productivity | No it does not | Im not aware what regulations I am supposed to be following | No | Yes, because it limits your interaction with the information at stake so we might not be able to finish a task sooner because of |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | certain processes that needs to be followed |
| IQ 2.4.1) | Do you think protection of information is part of the organisation's strategy? | I don't know | Yes it is as we need to protect our assists | Yes to ensure competitors don't have access to their clients | Yes probably im not very sure on it | Yes | Yes, they need to ensure that information is protected , because they can get sued if information have been corrupted or leaked. |
| IQ 2.4.2) | Do you think the organisation evaluates past security experiences? | I don't know | Yes we do asses and try and improve go forth | Yes to improve | Im sure any organization will it makes sense | Yes to prevent any breach | Yes, that is how an organization would improve on its securities and regulations. |
| IQ 2.4.3) | Does your organisation have a data backup and disaster recovery plan? | I don't know | Yes we do | Yes | I don't know | Yes | Yes, they would have an information (data) recovery plan, it forms part of compliance. |
| IQ 2.4.4) | Are risk vulnerability checks constantly conducted in your organisation? | I don't know | Yes on regular basis to ensure compliance | Yes to ensure all regulations are met | I don't know never heard of it | Yes | Yes, to identify possible threats and breaches in the system. |
| IQ 2.4.5) | Is creating user awareness on security threats is part of education and training for the organisation? | I am not sure | Yes it is | Yes | We get induction when we start to make us aware | No | Yes, employees need to be educated on security threats and breaches in order for them to comply with rules and regulations in case such an event occurs. |

| | | Interviewee 13- Admin clerk, Middle, Admin | Interviewee 14- Training clerk, Middle, HR | Interviewee 15- Research manager, Senior, Research | Interviewee 16- IS Manager, Senior, IT | Interviewee 17-Admin Clerk, Low, Admin | Interviewee 18- Legal clerk, Middle, Legal |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 1.1.1) | Does the FSB and government ensure your organisation complies with regulations? | Yes because they are our regulator | Yes in order to do business we have to | Yes in order to be a legal business we must comply | Yes in order to obide by the law | Yes I think they do | Absolutely not only does our company have audits that make sure that we comply with all rules and we also abide by south African working laws. |
| IQ 1.1.2) | Do you have specific corporate compliance approaches/strategies? | I'm not sure but I think we do | I wouldn't know, was never told | Yes we have many like fica and fais also we employ a compliance officer to assist us in this regard | Yes we do, fica is one of them | I don't know im not a part of it | absolutely – we try to keep our company as unique as possible and a very good environment to work in – we try to keep things on a more casual but professional manner. |
| IQ 1.1.3) | In your opinion how well are your information security policies enforced? | I think fairly well | I think quite well | I think fairly well | I think they are fairly well enforced | In my opinion I think good | very well most of it, is top secret – regarding financial – and we follow strict rules that we make sure we and the entire company abide by or else we follow disciplinary. |
| IQ 1.1.4) | Does your organisation comply with regulation because of industry standards? | Yes in order to keep up | No we comply because we have to | Not only because of industry standards but it is one of the reasons and it does have some influence | Yes we have to keep up with industry in order to remain competitive | I don't know never came across or seen any evidence so I wont be able to give an answer | Yes on this aswell as we do follow south African work laws. |
| IQ 1.2.1) | According to you what are the major factors considered in complying with the regulator? | Customers and information | Probably correct information | Accurate information | Information security, fraudulent behavior | I don't know | Major factors – would be making sure you follow everything by the book and comply or else we would be penalized. We could face heavy fines by not complying..so we have to follow everything by the book. |
| IQ 1.2.2) | What challenges are you experiencing when facing these factors to an attempt to comply? | Difficult customers and wrong information | Accurate information | Submitting the right information and obiding by regulations that affect our business | Having all the information available during audits | Im not sure and cant say exactly | Its challenging in the sense that everything has to be by the book, but im already groomed into this mindset and apply as far as I can – my challenge is |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | to keep myself up to date with the latest regulations. |
| IQ 1.2 3) | How do you overcome the challenges you are facing? | With the help of management | Aim to get the most accurate information we possibly can | With the assistance of Information Systems and the implementation of better business processes | We work hard in order to comply by improving our information system processes | Ive never faced any before | by keeping up to date with the latest regulations and grooming myself into the mindset of compliance. |
| IQ 2.1.1) | Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security? | Yes we must protect our information for all stakeholders | We must ensure that the consumer feels safe enough to trust us | Not only because of this but it does have an influence | Yes that is another reason we have to comply so that our clients can trust us with their money | I don't know | Yes, we do it for the sake of consumers and to protect their rights and privacy. |
| IQ 2.1.2) | How do regulations and policies influence your organisations information's security? | Makes it more tighter | They are used as guidelines | They influence it in a positive way | They positively influence it by ensuring we follow effective guidelines | I don't know | It makes people think twice before they step out of line or don't follow procedures because they are aware of the implications. |
| IQ 2.1.3) | What role does management play in implementation of information security compliance? | They need to oversee that everything is being complied with | They are there to enforce the guidelines | They are there to make sure their respective departments comply | We ensure our department complies to security measures and policies | Im not completely sure on what role they play | Management usually brings the message across to staff (in our workplace) – and they are the 1's to bring out disciplinary if the lines are crossed. |
| IQ 2.2.1) | Are you regularly informed of any changes in compliance requirements ? | Not really, don't know | Yes we are to keep up to date | Yes in order to make sure my department complies | Yes I am in order to update my department | Yes I am only things pertaining to my job | Yes. The company does this to make sure that everyone is aware and to make sure that staff complies with it – we normally get communicated via mail. |
| IQ 2.2.2) | Are you are aware of the risk of non-compliance? | Yes I think the organization would be fined or suspended to do business | No not specifically | Yes I am in order to avoid it | Yes I am so that I may reduce the risk of it ever happening things such as fines or penalties and in worse case in could lead | No I am not I just know that we must do it to be able to do business | Yes. We could face disciplinary. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | to prosecution | | |
| IQ 2.2.3) | What do you do when faced with information security problems? | Escalate it to manager | I raise it with management | I call on IT | We resolve it | I call IT | I implement as far as I can and make sure I don't step out of line or otherwise id face disciplinary. |
| IQ 2.2.4) | Do you access information that is not meant for you? | No its not meant for me so I don't need it | No I do not it's not meant for me | No its not meant for me | Yes it falls in my job description as I deal with all of the organisations data | No I can't get to it | Yes im guilty, I have access to the entire sites information some not meant for me too, but I will take a look, just to know whats happening inside the company. |
| IQ 2.2.5) | Do you know of any rules or regulations that exist around information? | Not really, don't know | We must have permission to check a persons information | Yes, fica and protection of personal information | Yes protection of information, fica, electronic communications act etc | Privacy laws | Yes I do as it falls in my job description |
| IQ 2.2.6) | Who is responsible for the security of your organizations information? | IT | IT | Management and IT | Everyone from the BOD to the secretary | Privacy laws | IT |
| IQ 2.3.1) | Do you think observing, tracking and notification of security incidences are part of your daily work routine? | There are enough security controls I think | No, It doesn't happen often | No not really but when an incident does occur we deal with it immediately | Yes it does in order to reduce the risk of it which falls under my responsibilities | It does not form part of my routine | Absolutely it makes you aware of what you should do and what you cant do..its a good guideline for me |
| IQ 2.3.2) | In your opinion does complying with policies and regulations hamper your productivity? | Sometimes depending on the task | Yes it does but we must do it to comply | No it comes part and parcel with the job | It's part of my job it needs to be done theres no way around it | No I don't believe so | Not actually, policies and procedures we review in our spare time, which does not affect my work productivity. |
| IQ 2.4.1) | Do you think protection of information is part of the organisation's strategy? | I think it's considered but not part of its strategy | I wouldn't know | Yes our information is very important and it must be protected | Yes. Our information is our most important asset | Yes I think so | Ofcourse. Especially ours because we have so many competitors that we don't want our information leaked out too, this is what sets us apart from our competitors we |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | **are unique in our policies and strategies which is highly confidential.** |
| **IQ 2.4.2)** | **Do you think the organisation evaluates past security experiences?** | **Most probably to ensure it doesn't happen again** | **Yes I think they do it's good to learn from mistakes** | **Yes it would be stupid if we didnt** | **Yes we do in order to mitigate our risks** | **Yes I think so to better the organisation** | **yes all the time – we always have a review of past experiences, sometimes to see what we can improve on and what we can still keep – we are big on this notion and have constant meetings around this** |
| **IQ 2.4.3)** | **Does your organisation have a data backup and disaster recovery plan?** | **Yes they do** | **Yes most probably** | **Yes we do in order to reduce our risk and it is a requirement from the regulator** | **Yes we have a disaster recovery offsite** | **Yes we have a DR site** | **Yes. Being part of the team my job is to also make sure our data backup is in tact and to make sure all information is correct and nothing is lost on our database.** |
| **IQ 2.4.4)** | **Are risk vulnerability checks constantly conducted in your organisation?** | **Im not sure** | **I wouldn't know** | **Yes our head of IT would make sure of that** | **Yes we perform them regularly** | **I wouldn't know hey** | **Yes. Very highly, because we are a financial company – we always evaluate risks / costs – because 1 wrong move could cost the company millions – and that's why we have to carefully strategise** |
| **IQ 2.4.5)** | **Is creating user awareness on security threats is part of education and training for the organisation?** | **No only when and if a security incident happens would we be told about it after** | **Yes when and if it happens** | **Yes we give our employees training in our induction program** | **Yes we try to train users on how to reduce threats in the organisation** | **No we never do training on it** | **in our company it's a huge awareness =- as one of our main aims is education – its something we pride ourselves on. So we are constantly reminded of the threats around us.** |

| | | Interviewee 19 - Finance Clerk, Middle, Finance | Interviewee 20- HR clerk, Low, HR | Interviewee 21- Legal clerk, Middle, Legal | Yes/No | Summary | Themes |
|---|---|---|---|---|---|---|---|
| IQ 1.1.1) | Does the FSB and government ensure your organisation complies with regulations? | Yes they do it's the law to do business | Yes I think they do | Yes, they ensure that the investing community are protected from a range of factors that could put a customer in financial difficulty. | 18 yes 3 no | Most employees knew that their organisation has to comply with regulations from either government or a regulatory body. The minority of people who did not know were low level employees such as the secretary | compliance - regulations |
| IQ 1.1.2) | Do you have specific corporate compliance approaches/strategies? | Im not sure what they are | I don't know im not involved in it | Not sure what they are exactly | 11 yes 10 no | Half of the people knew that their organisation has compliance approaches or strategies which the follow to reduce risk and half did not know and was unaware of it | compliance -strategies |
| IQ 1.1.3) | In your opinion how well are your information security policies enforced? | I think they are enforced well although I don't really notice them | I think they are enforced well im not sure its only my opinion | On a scale of 1-5 I would say 4, as we have had no auditing complaints as of yet. | 19 well 2 don't know | According to most of the employees they believe that information security policies are enforced well in their organisation | compliance |
| IQ 1.1.4) | Does your organisation comply with regulation because of industry standards? | I think they comply to not be fraudulent | Im not sure I don't really know | Compliance is because of the FSB. | 10 yes 11 no | Half of the employees did not now the reason for their organisation complying to regulations and half of them answered to what they thought the reason was | knowledge |
| IQ 1.2.1) | According to you what are the major factors considered in complying with the regulator? | I don't know, I don't deal with the regulator | I don't know its never been communicated to me | Reckless information | 6 did not know and the rest gave what they think the factors are | A few employees did know know what the major factors were while most of the other employees answered to the best of their | knowledge |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | knowledge | |
| IQ 1.2.2) | What challenges are you experiencing when facing these factors to an attempt to comply? | Im not sure | I don't know either | Enhancing the system to accommodate regulations in a very short period of time. | 7 did not know and the rest gave their challenges | A significant amount of employees did not know the challenges they face when complying while more than half gave their challenges they they experience all being different from eachother with no general answer | Knowledge |
| IQ 1.23) | How do you overcome the challenges you are facing? | I ask a colleague | Im not sure | Compliance is top priority so reassigning internal resources. | 5 did not know and 16 used different methods | A quarter of the employees did no know how to overcome their challenges to comply while three quarters used different methods respectively to overcome them | Training |
| IQ 2.1.1) | Does your organisation comply with regulation because of the consumer and stakeholders expectations for privacy and security? | Yes they are the customers and they need to trust us | I don't really know | To my knowledge compliance is initiated from the FSB and they have privacy and security concerns to protect consumers | 4 did not know and 17 knew | A few employees did not know while most of them answered yes consumer and stakeholders expectations does influence compliance. There were a few employees who disagreed and said they comply for other reasons | Compliance - |
| IQ 2.1.2) | How do regulations and policies influence your organisations information's security? | Im not sure on that | Im not sure | It influences the protection of a customer's personal information. | 6 did not know and the rest said its positive | More than three quarters of employees believe regulations and security policies has a positive influence on information security in their organisation | security-regulations |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IQ 2.1.3) | What role does management play in implementation of information security compliance? | They are ultimately responsible for it | I don't know unfortunately | Management is the driving force behind any sort of compliance. | 4 did not know and 16 answered | Most of the employees believed that its managements responsibility to enforce security policies and regulations. A few employees did not know | responsibility |
| IQ 2.2.1) | Are you regularly informed of any changes in compliance requirements ? | Yes most times | I don't think so | Yes, I am responsible for the design of system enhancements and compliance can have an effect on the system. As for security compliance – not sure. | 4 does not and 17 does | A few employees believes they are not informed of any changes in compliance requirements because their job does not require them to know and all the others believes they are informed appropriately most of the time | Communication knowledge |
| IQ 2.2.2) | Are you are aware of the risk of non-compliance? | Not really just know that it's not good for the business | Not really I don't think I need to know | Yes, I make it my duty to be informed as it could have an impact on my personal financial status. As for security compliance – not sure. | 8 did not know and 11 did | Half of the employee were unaware of the potential risk of non compliance to security policies or regulations.They did not know of the consequences of non compliance. Most of the other half gave their opinion but were not fully aware as everyone gave different answers | Compliance -knowledge |
| IQ 2.2.3) | What do you do when faced with information security problems? | I take it up with IT | I call my manager | I would normally consult with the enterprise architect | 11 escalate to management, 3 to IT and 1 to compliance the rest tries to resolve it themselves | More than half of the employee escalates any information security problems to their managers. A seldom amount contacts IT and the rest tries to resolve the problem themselves | security |
| IQ 2.2.4) | Do you access information that is not meant for you? | No not really | No I don't its not meant for me | No, it is unethical | 1 person because its in his job, 1 person interset sites, the rest, 18 does not acess info | Only one person admitted to accessing information not meant for him. One accesses it because it | security - access |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | not meant for them | falls in his job description while all the others said they do not access any information not meant for them | |
| IQ 2.2.5) | Do you know of any rules or regulations that exist around information? | Yes, Fica | No I don't | I do know that personal information must be protected | 5 does nto know specific laws and 16does know something | A significant amount did not know of any laws surrounding information while more than half knew something it may not be all relevant laws | knowledge |
| IQ 2.2.6) | Who is responsible for the security of your organizations information? | IT | IT | IT | 1 compliance, 1 everybody,2 management, 1 privacy laws, 16 IT | 3 quarters of the employees said it is solely IT's responsibility to secure the organisations information. One said it was the compliance department. One said it was everybodys responsibility and another said it was privacy laws | security responsibility |
| IQ 2.3.1) | Do you think observing, tracking and notification of security incidences are part of your daily work routine? | No I don't think so | No I don't think so not sure | Maybe, as the information processed by the functionality of the system must be processed securely. | 12 no,1 maybe , 7 yes | More than half said that tracking security incidents is not part of the daily routine. A few said yes it is while one said maybe if it happens | Security responsibility |
| IQ 2.3.2) | In your opinion does complying with policies and regulations hamper your productivity? | Yes it does but its necessary | No I don't think so | No, pressurized projects are the most fun. | 11 no, 2 I don't know , 7 yes but necessary | Just over half of the employees said complying does not hamper their productivty while 2 employees did not know and the rest saying that it does hamper their productivity but they have to do it | compliance - productivity |
| IQ 2.4.1) | Do you think protection of information is part of the organisation' s strategy? | Yes it should be im not 100% sure though | I don't know | Yes, compliance is top priority. | 1 no, 4 don't know, 16 yes | Most employees believe that protection of information forms part of the organisations strategy. A seldom few did not know while | strategy |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | one employee siad that its not | |
| IQ 2.4.2) | Do you think the organisation evaluates past security experiences? | Im sure they do | I don't really know hey | Yes it is standard practice to learn from past experiences. | 3 dont know, 17 yes | A significant amount of employees believe that the organisation evaluates past security experiences in order to reduce the risk of it happening again. A few did not know | security - risk |
| IQ 2.4.3) | Does your organisation have a data backup and disaster recovery plan? | Yes they do to protect the information in case of a natural disaster | Yes I believe we have a DR offsite for that | Yes, if customer's information were to be lost it could lead to a non –profitable business resulting retrenchment | 2 don't know, 19 yes | Most of the employees agreed that they do have a backup plan and said to have a DR offsite | risk-dr |
| IQ 2.4.4) | Are risk vulnerability checks constantly conducted in your organisation? | Im not sure im not part of IT | I don't know | Yes, in order to sustain the company. | 11 don't know, 10 yes | Half of the employees believes there is vulnerabiliity checks conduted in the organisation while the other half said they either are not aware of it or they do not | security - risk |
| IQ 2.4.5) | Is creating user awareness on security threats is part of education and training for the organisation? | Yes when we start to work in induction | No, I think it is for certain people | To my knowledge, No. | 6 no, , 15 yes | Most employees said they received training upon entering the business but never again. A few people also said that security training has not been given to them | training |

## Appendix 3: Consent letters: examples of company and participant consent

Cape Peninsula
University of Technology

Date: 10 May 2014

To whom it may concern.

This letter serves to confirm that Mr. Reza Desai, student number 205219500 is currently involved in formal research as part of his M Tech (IT) degree here at CPUT. His topic concerns "An integrated approach for information security compliance in a financial services organisation". Please ask to see his student card to confirm his identity.

As his research supervisor, I would be grateful if you would allow him access to interview you as he requests. He understands the ethical issues associated with interviewing employees in an organisation, and I will be keeping a careful eye on both his approach to the interviews and on the questions he asks.

You are welcome to at any time before, during or after the interview, ask that the interview be cancelled and that the results of the interview may not be used.

His research should be concluded by the end of December 2015.

May I ask that you please sign this document as proof that the student did inform you of the research, its use and the opt-out option?

Thank you.
Regards

Dr AC de la Harpe
Supervisor
082 448 1058
021 460 3627

.....
Interviewee

T. GARELDIEN.
.....
Print initials and surname.

OASIS

GROUP HOLDINGS (PTY) LTD.

OASIS HOUSE · 98 UPPER ROODEBLOEM ROAD · UNIVERSITY ESTATE · 7925 · SOUTH AFRICA
P.O. BOX 1212 · CAPE TOWN · 8000 · SOUTH AFRICA
TEL: 27-21-413 7860 · FAX: 27-21-413 7900 · EMAIL: info@oasiscrescent.com · WEBSITE: www.oasiscrescent.com

**Consent letter** **27 February 2014**

I Natheer Firferey , in my capacity as IT Manager at Oasis Group Holdings give consent in principle to allow Reza Desai, a student at the Cape Peninsula University of Technology, to collect data in this company as part of his M Tech (IT) research. The student has explained to me the nature of his research and the nature of the data to be collected.

This consent in no way commits any individual staff member to participate in the research, and it is expected that the student will get explicit consent from any participants. I reserve the right to withdraw this permission at some future time.

In addition, the company's name may or may not be used as indicated below. (Tick as appropriate.)

| | Thesis | Conference paper | Journal article | Research poster |
|---|---|---|---|---|
| **Yes** | | | | |
| **No** | X | X | X | X |

Natheer Firferey
Tel: 0214137979
Email: natheer@za.oasiscrescent.com