The Management of Risk Awareness in Relation to Information Technology (MERIT)

Khalid Bin Ishaq Alseiari

A thesis submitted for the degree of Doctor of Philosophy

University of Gloucestershire

Department of Computing and Technology

Faculty of Media, ART and Technology (MAT)

2015

ACKNOWLEDGEMENTS

There are several people who helped and supported me to complete this research. The Abu Dhabi Police General Head Quarters who financed my study deserve my unreserved thanks for supporting me to develop myself through research and enhance my career prospect. Thank you to my generous supervisor Dr. Kevin Hapeshi for all the valuable advise and guidance he provided throughout my research. Dr David Wakeling too who contributed supportive advise. The research committee who reviewed my research proposal provided informed guidance for which I am thankful. I thank my family for their complete and loving support.

I declare that the work in this thesis was carried out in accordance with the regulations of the University of Gloucestershire and is original except where indicated by specific reference in the text. No part of the thesis has been submitted as part of any other academic award. The thesis has not been presented to any other education institution in the United Kingdom or overseas.

Any views expressed in the thesis are those of the author and in no way represent those of the University.

Signed..... Date.....

Abstract

Current business environments are characterised by a wide range of factors and issues which combine to create an unprecedented level of uncertainty and exposure to risks in IT management and all areas of strategic and operational activities. However IT risk awareness presents both a problem and an opportunity to achieve effective IT risk management. This context creates an imperative for conceptualising risk awareness to account for the intensity, diversity and complexity of IT risks ensuring a heightened level of awareness. The central focus of this study is founded on the premise that IT risk awareness among individuals in all levels of the organisation is critical and involves consideration of human and social factors. The research aimed to evaluate current practice in IT risk awareness in police forces and explore what police forces in the UAE can learn from the best practices of other UAE public and private enterprises. The study further aimed to develop a new holistic conceptual model of IT risk awareness supporting IT risk management. Quantitative and qualitative data was collected to achieve the research objectives utilising three main techniques of structured survey, a Delphi method and in-depth interviews. The findings underline that IT risk awareness is not being maximised or embedded in UAE organisations and there is a lack of formalisation of risk management processes. Although the ADP particularly demonstrated these weaknesses this was also reflected to a lesser extent in other UAE organisations. The results show that a diverse level of knowledge in relation to risk awareness and management is evidenced and detailed knowledge of risk management was weak in addition to low awareness of policies and guidelines. Moreover IT risk awareness and management was perceived as solely the domain of IT departments and not as a collective responsibility. A further key finding is validation of all five components of Governance, Compliance, Enterprise, IT GRC and Risk management within the MERIT IT systems risk awareness model, affirming that it is appropriate and important to examine risk awareness in relation to these elements. Model components were further found to be iterative and interdependent and findings highlighted the critical role of governance in facilitating risk awareness and other elements in the model. Finally, risk awareness is found to be critically underpinned and influenced by a complex range of different elements involving cognitive, social, cultural, emotional and psychological aspects in addition to the extent to which people understand a range of different types of risk. The MERIT model provides significant opportunity to identify, assess and address these elements.

CONTENTS

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Background and Context

Today's business environment is characterised by a wide range of factors and issues which combine to create an unprecedented level of volatility, uncertainty and exposure to risks in IT Management and all areas of strategic and operational organisational activities. IT risk awareness presents both a problem and an opportunity to achieve effective IT risk management. However the issue is heightened as organisational employees including managers often lack awareness of threats to IT systems and appropriate security measures (Hoffer and Straub, 1989; Goodhue and Straub, 1989; Straub, 1990; Ceraolo, 1996; Straub and Welke, 1998; Sipponen, 2000).

Risks to an organisation's operational IT systems or mission-critical information systems, defined as transaction processing systems, can be critical and significantly disrupt business or government agency operations. Such threats arise from external sources such as terrorists, industrial espionage or state-sponsored espionage, which recently has included threats from the Russian and Chinese states. The threats can also be from internal sources, such as disgruntled employees or ex-employees and can target organisational IT systems directly or via the Internet. Vast private and public databases are attractive targets emphasising calls for 'information disaster planning.' Pember (1996) first argued that information disaster planning should be an integral aspect of an organisation's risk management strategy.

Information risk management is the protection of an organisation's IT architecture and information infrastructure: Pironti (2012, pg.1) states that: "It identifies the business value, business impact, compliance requirements and overall alignment to the organisation's business strategy". Organisations are exposed to a wide range of IT risks with recent examples of e-risk including police officer collusion with private investigators on the orders of criminal gangs to access national police computers and databases to delete records of criminal investigations and extract other information (Channel 4, 2012); leaking of US Embassy Diplomatic Cables (Cablegate, 2011) and social security data loss by the UK government. Attacks on computer systems through viruses and a wide array of malicious and fraudulent software is another significant area of risk which has multiplied exponentially for organisations. An unrelenting and continuously evolving pattern of computer attacks by

hackers from around the world creates risk to data access, theft and corruption for all organisations. The UK government's Home Office website was hacked into by the 'Anonymous' group of hackers who denied users access to the website (BBC, 2012). In another example five million emails of global intelligence firm Stratford were made public. The firm provides confidential intelligence services to large corporates, such as Dow Chemical Co., Lockheed Martin and government agencies (TGIF, 2012).

1.2 Risk & Risk Management

This context creates an imperative for conceptualising risk awareness to account for the intensity, diversity and complexity of IT risks toensure a heightened level of awareness contributing to effective risk management. Broadly the notion of risk refers to a situation where individuals or organisations are exposed to a threat or danger characterised by uncertainty and potentially adverse impacts (Machina and Viscusi, 2013). The Institute of Risk Management broadly defines risk as an amalgamation of the likelihood of an event occurring and its resulting positive or negative outcome (IRM, 2002). The measurement of risk can be traced back to as early as the 1700s and the idea that subjective beliefs could be objectively understood was Bernouille's unique contribution to understanding and development of knowledge of risk (Bernstien, 1998). It is this subjective belief and its role in IT risk management that is investigated in this research, described as IT systems risk awareness.

Risk awareness underpins one of the primary stages of risk management, risk identification. This is contingent on in-depth understanding of the organisational internal and external contexts such as legal, political and cultural factors. Risk management is the process by which risks in relation to the achievement of organisational objectives are identified, quantified and managed (Hickson and Owen, 2015). Planning, identification and analysis of risk are key stages in this process culminating in the development of response strategies, monitoring and control (Kerzner, 2009).

1.3 The Importance of Risk Awareness

Risk awareness is knowledge of the nature, dangers and probabilities of risk occurring in particular situations (ACCA, 2007). A fuller description depicts risk awareness as a mental process involving images developed on a personal or collective basis in relation to existing

hazards. These images are applied to inform vulnerability self-awareness and the relationship between both dimensions. Risk awareness can therefore be viewed as an active interpretation of risk and is argued to be an element of risk itself (ISDR, 2006).

The central focus of this thesis is founded on the premise that IT risk awareness among individuals in all levels of the organisation is vital to improving the effectiveness of IT risk management strategies. These researchers call for techniques to increase individuals' IT risk awareness as part of overall IT risk management. The research reported is aimed at understanding individuals' IT risk awareness, from an enterprise-wide or organisational perspective and develop metrics to measure the IT risk awareness of individuals. There is a danger that risk awareness occurs in a haphazard manner rather than within a strong risk awareness culture based on robust frameworks and measurement.

Risk awareness can be viewed as a fundamental building block of effective risk management. It is newly proposed and intended to facilitate our understanding of staff responses to manifestation of negative incidences through the reliance on the practical knowledge, awareness and professionalisation of all staff members. Such capabilities rely on some understanding of human factors as well as products and services being provided. Employees will be capable of recognising and responding to early signs of impending crisis, or be informed enough to play their respective part in a more sudden manifestation of crisis. Risk management is dependent on the awareness of all types of risks faced by organisations in order to ensure appropriate and effective measures. Risk awareness is a combination of *vulnerability assessment* and *knowledge management*, which provides critical input to the Risk Identification process within the overarching Risk Management framework (Gibson, 2003). Therefore, each enterprise must develop their own awareness schemes and policies to identify and understand what could go wrong, and additionally develop crisis management strategies, particularly for unforeseen negative incidents.

The role of risk awareness as the basis of risk management is increasingly noted in the literature. Deluccia (2008) points to its significance for accurate identification of potential threats as the basis of effective responses. This is notably more so given the shift from a relatively stable and consistent economic business environment towards the modern dynamic capitalism characterised by factors such as social and economic liberalisation, a primary factor which highlights the significance and challenge of maintaining risk awareness. The

rapid, complex and continually evolving nature of today's business and social environment is widely debated in the literature. Hopkins (2013) points to a wide range of dynamic and diverse prevailing issues underlining the significance of risk awareness and effective risk management systems. Today's marketplace is characterised by a fast changing business environment and increasing competitive forces, globalisation of demand and supply factors and changes in consumer behaviour including heighted expectations and reduced brand loyalty. The rapid changes in technology and reduced product lifecycle have intensified the focus on continuous product development and innovation. Such changes in the marketplace create increased pressure to commit to bolder strategies and reduced timeframes for success in order to remain competitive (Thamhain, 2014). Meanwhile, the increase in civil unrest and conflict around the world coupled with the increase in environmental events caused by extreme weather conditions creates a further dimension of risk which can impact organisations in diverse ways.

The environment confronting risk managers is volatile, wide-ranging and complex presenting major challenge to align and comply with multiple and continuously evolving regulatory regimes (Kalinich, 2013). Moreover the borderless nature of advancing technologies such as the internet challenges national jurisdictions leading to significant confusion in discerning appropriate compliance (Jain and Kalyanam, 2012). Failure to address any of these issues can result in reputational damage, regulatory penalties, loss of crucial data or intellectual property and significant business costs (ENISA, 2012). This underlines a significant imperative for risk managers to comprehend and maintain pace with the fast-moving risk environment and for organisations to ensure and prioritise risk awareness across all levels of the enterprise. Today's management issues relate to a broad range of challenges that expose organisations to a plethora of threats including variability of cost and availability of raw materials; complexity in supply chains; regulatory changes and the growing significance of intellectual property (IP). Globalisation further exacerbates these challenges in operating across multiple borders and complying with often divergent national systems and cultures. The increased pace of and dependency on technology and the prevalence of e-commerce are further major factors which generate myriad risks for organisations. The increased role of managed services or third party providers implies another layer of associated risk arrangements and requires increased cognisance of risks related to IT arrangements of data safety, privacy and compliance (Dunkerley and Samuelle, 2014). This context emphasises the importance of risk awareness

on many levels and in many areas and heightens the need to understand specific risks. This context further underlines the significance of risk awareness as a continuous process model.

1.4 Research Problem

Before one can address a risk it first must be recognised and this is the central dilemma this thesis aims to address. It is highly questionable given today's context whether an effective level of awareness and risk awareness culture across all functions of the organisations promotes discovery of risks and alignment of processes to address risks. Firstly, the role of risk identification has in the past been centred on senior personnel which today needs to shift a less localised and more pervasive activity which draws on the vigilance, knowledge and expertise of all employees. However an understanding of processes, issues and critical components to achieve this is lacking.

IT is associated with significant financial risks emphasising the importance of addressing risk within IT systems. Earl (1996) considered how managers make decisions to outsource IT systems and contends that managers should consider why they should not insource. He identified eleven risks associated with IT outsourcing including: possibility of weak management in the Seller Company, inexperienced staff, business uncertainty and hidden costs. One particular risk, 'endemic uncertainty', concerns IT operations and development as 'inherently uncertain'. "Users are not sure of their needs, new technology is risky, business requirements change, and implementation is full of surprises" (p. 29) This provides an insight into the problematic manner of managing IT systems risk in the context of inherent uncertainty. Jourdan et.al, (2010) further report that: "the results also show that organisations still have room for improvement to create idyllic ISRA processes" (p.33) – Information Systems Risk Assessment (ISRA). They identified eight risk factors, with financial loss (93%) and risk to infrastructure (81%) accounting for the highest focus. Firm theoretical basis for IT systems risk management strategies involves deterrence, prevention, detection and recovery (Straub and Welke, 1998).

The need for information system risk awareness is critical given the increasing range and number of risks to which information systems are exposed on a daily basis. The problem is pervasive with over 90% of US companies for example experiencing some type of cyber-attack and the global cost has been conservatively estimated at approximately $388 billion (Hampton 2014; Hopkins, 2013). The nature of the threats to information systems are diverse,

dynamic and evolving and include attacks such as denial of service, phishing, data breaches, and deployment of malware, malicious code and botnets. These attacks are frequently designed to support the execution of cyber-crimes involving wrongdoing such as theft, fraud and extortion of organisations (Jain and Kalyanam, 2012).

Furthermore, the subjectivity of risk awareness is a challenge which has yet to be addressed in the literature. Risk management strategies that focus solely on the assessment and measurement of objective factors are less effective because they overlook the people or social aspects of risk management. Whilst quantified studies of risk and risk management have been conducted and problems with quantification discussed in both IS and other disciplines (Haber, 2011; Huges, 2009; Arend, 2012; Ikram, 2000; Straub, 1990), there is little quantitative research on the subjective IT systems risk awareness of employees. It is employees who need to become aware of risk and need to remain vigilant of risk in order to recognise the vulnerabilities of the organisation, and prevent threats or attacks on IT systems. Management need metrics on peoples' subjective awareness of the risk faced by organisations in order to formulate and evaluate the effectiveness of their IT systems risk management strategies.

In the context of widespread use of IT by organisations, IT risk management needs to be understood from both the perspective of the computer hardware, software and, crucially, from the perspective of the people who use IT and information systems (IS). The risk exposure of the computer hardware and IT systems can be measured using metrics specifically developed to assess threats to computers and software IT systems. These include metrics used in other domains such as volatility, compliance, terror and or systemic risk (Haber, 2012). But the risk exposure of the people who use the IT systems and IS is subjective. Research on the subjective aspects of IT risk management is lacking however this is an important gap as people are the central feature and potential weakness of any business process-oriented IT system.

However, existing research does not account for individuals' IT risk awareness as integral to IT risk management. The Risk Management Guide for Information Technology Systems states that: "Risk is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability and the resulting impact of that adverse event on the organisation" (NIST, 2002). Information technology is digital technology that enables

organisations to collect, store and processes data in electronic format to provide valuable information about products, services and customers, as well the internal operations of the organisation. The potential vulnerabilities or challenges to such IT systems are data loss, media damage, stolen data and inaccessibility of information and data (Data, 2006). The NIST definition of risk above does not recognise the importance of the personnel (management and staff) within the process of risk management. Employees' basic principles, beliefs, perception, values and attitudes all contribute to the composition of an organisation's risk culture. Bowen (2006) has suggested that the 'human' factor is critical for effective IT risk management. It is people who are the most vulnerable part of any plan or effort to minimise the risk potential from IT in an organisation. This has been highlighted by audit reports, periodicals and conferences (Epich and Persson, 1994; Bowen, 2006). Risk management strategies, manifested as policies and procedures, can only be effective within an appropriate risk culture. Furthermore, the NIST definition does not recognise the unique requirements of police forces and their IT systems and administration, which is where the present research was conducted to understand IT risk management.

The lack of conceptualisation of risk awareness undermines the ability of organisations to measure and raise risk awareness for individuals, teams and organisations to a level necessary to address mission-critical objectives. It is this problem which forms the focus of this study. Through critical evaluation of the literature, this research develops a conceptual model of IT systems risk awareness consisting of five elements drawn from the extant literature. From this conceptual model derives the **M**anag**e**ment of **R**isk Awareness in **R**elation to **I**nformation **T**echnology (MERIT) conceptual model to understand the risk awareness of IT systems of employees in organisations.

1.5 Research Questions

Consequently the focus of this study is underpinned by the following research questions:

1. What is the current practice in IT risk awareness in police forces?
2. What can police forces in the UAE learn from the best practices of other public and private organisations in the UAE such as banks and multinational oil companies?
3. What aspects of risk awareness can inform a new conceptual model of IT risk awareness in high priority IT risk management duties and responsibilities?

1.6 Research Aims

This research focuses on understanding peoples' risk awareness to develop better formal or mathematical understanding of risk awareness. This involves consideration of behavioural aspects of IT risk management by understanding employees' IT risk awareness. The literature review reveals that to date there has been no behavioural research seeking metrics for assessing IT risk awareness from the behavioural perspective. Therefore, this research aims to develop metrics to gauge risk behaviour or risk awareness by developing a new enterprise-wide conceptualisation of IT risk awareness and to derive a model from this conceptualisation to define and understand IT risk awareness. The academic justification for the research aim is that it is necessary to understand and develop knowledge of the significant aspect of IT risk awareness in the overall management of IT risk. A review of the literature shows the lack of a conceptual framework for developing and assessing risk awareness. The practical justification for the research aim is that IT risk awareness is important because of organisational dependency on IT for routine operations and strategic purposes.

1.7 Research Objectives

1. To evaluate the current IT risk management practices
2. To identify by conducting a survey among IT managers, the current practice in IT risk management in order to explore and evaluate the extent of staff involvement in the management of risk in UAE enterprises.
3. To develop a new conceptual model of IT risk awareness in high priority IT risk management duties and responsibilities.

1.8 Research Methodology

The overall research design is based on a mixed method approach drawing on both positivistic and interpretivist research philosophies. While the predominant orientation is positivistic in gathering empirical data, an interpretivist dimension is incorporated to generate in-depth qualitative understanding of the research focus. Consequently, a mixed method case study based strategy combining quantitative and qualitative methods is employed applied to multiple cases. The research is based on three primary research methods: structured questionnaire survey, in-depth interview and Delphi expert panel.

1.9 Research Contribution

This research contributes to current knowledge of risk management by evidencing the importance and critical role of risk awareness in the risk management processes. The main contribution is enhancing the theoretical basis for IT Systems Risk Awareness in proposing an objective framework for developing and assessing risk awareness. Further, it enhances the theoretical understanding of risk awareness constructs in the risk identification stage in relation to maximising risk awareness culture. Generally, this study adds to the limited research on the conceptualisation and development of risk awareness in IT environments. The findings can emphasise the importance of risk awareness in today's IT context and provide guidance in addressing risk awareness using a structured approach.

Research impact can be economic or social. Research Councils UK (RCUK) defines research impact as "the demonstrable contribution that excellent research makes to society and the economy". This definition of research impact mentions 'demonstrable contribution'. Such contribution would perhaps result in improving economic performance and competitiveness of companies and increasing effectiveness of public services and policy. It is expected that the outcomes of this research will have clear impact on the practices of the United Arab Emirates (UAE) Police Force IT Department and therefore increasing effectiveness of public services. Through the sponsorship by the UAE Police Force of this research and their active involvement in the research process, it is expected that the output of this research, the risk awareness metrics, will improve the level of implementation of the assessment and management of risk to IT systems data and information in the UAE Police Force IT Department.

The outcomes of the research can be applied to practice. It is expected that the main outcome of the study, the MERIT IT Systems Risk Awareness model, will be used by the UAE Police Force to (a) help them better articulate their risk awareness policies, (b) provide appropriate training and (c) use IT support to enable accurate risk identification, control and mitigation. This outcome can be generalised to cover other Gulf Country Police Forces through specific and wider communication and engagement. The specific benefit to them will be bespoke formulation of the MERIT IT Systems Risk Awareness model and risk awareness metrics. The research will broaden the impact to benefit other Gulf Countries' Police Forces, who will be invited to share best practices. The research impact timeline over six months, in Table 1

below, indicates the ensuing expected outcomes of the research project in the UAE Police Force. The problem of risk awareness in the context of a risk management strategy will be addressed with colleagues in the Force. The MERIT IT risk awareness model will be applied in collaboration with the Force's risk management experts, which will further co-produce knowledge through its activities, outputs and usage

Table 1 Research impact timeline over six months

<table>
<tr><td colspan="3">Communication & Engagement & Involvement</td><td colspan="3">Exploitation & Application</td></tr>
<tr><td>Month 1</td><td>Month 2</td><td>Month 3</td><td>Month 4</td><td>Month 5</td><td>Month 6</td></tr>
<tr><td>Initial Communication & Engagement with the Force.</td><td colspan="2">Communicate MERIT IT risk awareness model to Force's Delphi Panel.</td><td colspan="2">Apply MERIT IT risk awareness model.</td><td>Monitor and evaluate MERIT IT risk awareness model in the risk management of the Force.</td></tr>
</table>

Direct immediate benefits will accrue to the Force which has a culture of utilising research knowledge. The specific benefit to the Force will be awareness of the need to have a risk awareness strategy using the MERIT IT risk awareness model. Force commanders and risk managers will benefit by considering this model to articulate their risk management strategy.

The research findings provide a basis to enhance policing practices in the UAE in a highly dynamic and rapidly changing environment through an objective understanding of risk awareness constructs. Such a framework provides a theoretical foundation for implementing risk awareness culture which maximises the knowledge and understanding of policing contexts contributing to heightened vigilance of signals in relation IT risks and appropriate responses.

1.9.1 Expected general outcomes

This research will add to the current knowledge of risk management by including risk awareness as a crucial important element in enterprise IT systems risk management. The MERIT IT Systems Risk Awareness model makes a contribution to measuring enterprise risk awareness.

1.9.2 Specific outcomes for UAE Police Force

To achieve professionalism within the Police Force's IT department in the UAE, the relevant experts and employees were consulted to assess the impact of the research on their practice. The UAE Police Force Department is actively supporting this research through funding and access to the phenomenon. They have been consulted to discuss the problem of risk awareness in IT systems risk management. Building relationships is an integral aspect of this research and the relationships will be continued after the funded research is completed. Our agreed two year projection is to change risk awareness policies and practices in the UAE Police Force and three year projection to fully implement the MERIT risk awareness methodology.

The research involved the following stages of communication with the UAE Police Force including: initial communication and engagement with UAE Police Force and IT Department; communicate MERIT IT Systems Risk Awareness model to UAE Police Force Directorate; communicate risk awareness metrics; validate risk awareness metrics among experts and monitor and advise on use of the MERIT IT Systems Risk Awareness methodology.

The impact timeline above corresponds with the outcomes of the project discussed with colleagues in the UAE Police Force. The problem of risk awareness was continuously addressed during the research in the various data collection stages and the phases of the research methodology outlined above. The research has collaborated with and co-produced knowledge through its activities, outputs and usage with and by the UAE Police Force. The dataset was collected in collaboration with the UAE Police Force and IT Department.

The development of the MERIT IT Systems Risk Awareness Conceptual Model was derived from theories of risk covered in the literature review. The principal impact will be on the way the UAE Police Force formulates and implements IT systems risk awareness.

1.10 Structure of the Study

The structure of the remaining chapters of this study begins with a review of the literature. Chapter 2 presents the theory in relation in risk and risk management identifying different major dimensions and concepts relevant to the study of risk awareness. This chapter draws on social theories and mathematical models on risk management to identify critical elements necessary to quantify risk awareness, defined as behavioural aspects of risk. Chapter 3 reviews the literature specifically in relation to risk awareness, IT risk awareness and dimensions of risk awareness. The research design is presented in chapter 4 commencing with a discussion of the philosophical approaches considered and the rationale for this study. This is followed by an explanation and justification of the research strategy and methods adopted. The results of the quantitative and qualitative data are presented in the subsequent chapters. Chapter 5 presents the results of survey data from Abu Dhabi police and multiple UAE case organisations, in addition to the results from in-depth qualitative interviews with representatives from both types of case organisation. Chapter 6 presents the results of the Delphi panel data. The results of the study are analysed and discussed in Chapter 7 which also places findings in the context of literature and explores the implications and significance of the results. The final Chapter 8 presents a summarisation of the study outlining the aim, key conclusions and theoretical contribution of the findings. A number of recommendations, and an outline of limitations and future research opportunities concludes this study.

.

Chapter 2: Risk and Risk Management

2.1 Introduction

This chapter provides an interdisciplinary review of the literature on the area of risk and risk management as the basis for conceptualising risk awareness. The aim is to define and identify theoretical, conceptual and prescriptive perspectives on risk management to establish the context for information systems (IS) and IT risk management in relation to risk awareness. Notions of risk, behavioural, sociological and systems theories are reviewed in addition to theories on risk management and risk assessment. This review therefore provides insights on the manifestation risk awareness associated issues. In addition the review provides an indication of linkages between risk awareness and risk management processes, guiding the development of a conceptual framework and criteria for this study.

The literature reviewed characterise both humanistic behavioural and rational perspectives impinging on risk awareness. Overall research on risk draws on social science theories of behaviour but appears to lack clarification of specific linkages between the invoked theory and its application to understand risk behaviour and management. The general deterrence theory is an example (D'Arcy et al., 2009). This is noted by Siponen (2000) who argues that other conceptualisations of risk and risk management, and conceptual frameworks for risk management, fail to establish generalisations in spite of drawing on theories of planned behaviour and reasoned action. The literature is predominantly centred on prescriptions or models of risk management that are argued to be applicable to practice. This review points to a notable gap in the conceptualisation of risk awareness.

2.2 Risk

The nature of risk is that it consists of consists of three elements: a threat, vulnerability and a risk, implying that if there are overlaps between the threat and vulnerability the result is the risk occurring (Coyle, 2002; Hiles and Barnes, 1999; Allan, 2007.) Hillson (2006) concurs that risk is an event which may occur in the future and which if it happens might impact on the ability of the organisation to achieve its objectives. Hillson and Newland (1997) define risk as an uncertain event or set of circumstances that, should it occur, will have an effect on the achievement of the project's objectives. Similarly, McNamee (1997) suggested risk is a concept that describes uncertainty in achieving goals.

It is evident that while risk has been defined in several ways a consistent element is the view that risk reflects the probability and magnitude of an occurrence of an undesirable event. On the one hand risk has been defined in relation to injury, damage, or hazards, while other definitions define risk in relation to occurrences which negatively impede the achievement of project goals (Hopkins, 2013). Mathematically it can be perceived purely as a quantifiable statistical probability of an undesirable event. These elements are associated with an objective view of risk. Different levels and categories of risk emphasise contextual dimensions of risk such as technical or performance risk concerned with the uncertainty which undermine the attainment of performance objectives (Machina and Viscusi, 2013). This diversity of the concept of risk underlines the importance of identifying the context and focus under study.

The perception of risk and inherent subjectivity significantly influences risk identification and management. Rosa (2003) points to a significant subjective dimension of risk underpinned by cultural and social factors that cannot be objectively determined. In attempting to reconcile the objective versus subjective views of risk Rosa (2003) defines risk as a "situation or an event where something of human value (including humans themselves) is at stake and where the outcome is uncertain" (p.56). This definition according to Rosa (2003) incorporates three elements consistent in all views of risk. Firstly, that risk represents a state of human reality, secondly, that an outcome is possible and finally, that it incorporates some element of uncertainty. In addition to the concept of probability Lam (2014) emphasises that a number of related concepts are associated with risk: exposure, volatility, severity, time horizon and correlation between risks These concepts shape the perception of risk in terms of

what is at stake, the degree of uncertainty, the length of exposure and the interrelation between risks. Risk can also be viewed in terms of three broad categories: hazards risks, control risks arising from uncertainty; and opportunity risks (Hopkins, 2014).

The conceptualisation of risk impacts on the design and implementation of risk management. Several definitions of risk management have been proposed. ISO defines it as "co-ordinated activities to direct and control an organisation with regard to risk" (Fraser and Simkins, 2010) while the Institute of Risk Management defines it as a "process which aims to help organisations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure" (Fraser and Simkins, 2010, p97). Hopkins (2014) provides broader reflection of risk management defining it as a "set of activities within an organisation undertaken to deliver the most favourable outcome and reduce the volatility or variability of that outcome" (p.37). Under both these perspectives there is an implicit assumption that users have an awareness of the risk factors in order to formulate decisions about appropriate processes or activities. Speed (2011) explains that risk management is underpinned by three key principles: proportionality, alignment and continuous change (Speed, 2011). The principles of alignment and continuity are in particular relevant in today's dynamic and interconnected business environment. These three principles suggest that a heightened sense of awareness requires an in-depth, concise and up-to-date understanding of the user context or situation in order to ensure measured responses which are consistently aligned with the environment.

Risk can involve a situation whereby the possibility exists that something damaging or fatal could occur, or the possibility of an event that could change from what was expected or planned. Risk occurs in business, government or other public organisations when they fail to manage properly (Aven and Renn, 2010). Therefore, it is the organisation that needs to be managed in anticipation of the uncertainty characterised by risk. Risk is referred to as a lack of predictability about problem structure, outcome or consequence in a decision, planning situation or design of organisations and systems (Aven and Renn, 2010). Risk involves the lack of information which leads to uncertainty; risk *mean*s both uncertainty and the result of uncertainty. Risk pervades society, economy, industry, government and individuals' lives (COSO, 2004). Tchankova (2002) argues that risk is an inherent part of business and public life. Borodizicz's (2005) view is that risk is a key question affecting every sphere of lifestyle, from diet to transport and power generation. Allan (2007) further argues that it is necessary to

establish what is meant by "risk" in order to work towards an understanding of risk management.

2.3 Psychological Theories of Risk

Two predominant areas of psychological theories of risk centre on cognitive and emotional factors in risk. Risk can be studied from a cognitive aspect which has been the earliest unit of analysis in research. A cognitive approach was originally applied to risk decision-making by Lopes (1987). Lopes (1995) propose that in risk decision-making information processing is different when appraising potential gains and losses (Lopes, 1995). This work indicates the potential role of other factors beyond the rational to influence decisions. Lopes identified 'risky choice' as behaviour affected by contextual factors influencing decision-making. This definition widens our understanding of risk as a purely rational decision-making process because it considers contextual factors. Later studies, discussed below, widen the scope even further by considering cultural and subjective factors.

2.3.1 Cognitive Risk

Psychological theory explains risk-taking as a rational decision-making process in which choices between alternatives with uncertain outcomes are considered based on probability of failure or success, and the benefit or cost of the risk (Assailly, 2012). Early theories attempted to explain such cognitive processes quantitatively however recent studies also acknowledge qualitative variables such as context and culture (Borodzicz, 2005).

Psychologists emphasise understanding how people perceive their environment; how they become aware of it, learn from it and act in it; this also gives such studies a behavioural aspect. This suggests that people's perception of their environment underpins their awareness of risk. This is underlined by how the brain deals with risk through cognition or the mental processes by which humans acquire knowledge through perception, reasoning and intuition (Mercantini and Faucher, 2015).

Several theories have been proposed which seek to explain how cognitive processes inform decision-making with relevance for risk choices. Kahneman and Tversky (2000) propose two decision-making stages known as prospect theory involving the mental creation of a frame of reference (framing) followed by the actual decision. This is supported by evidence indicating

that the way that individuals conduct framing can be impacted by personality (McElroy et al., (2007; Benjamin et al., 2007). A person's awareness of IT risk could therefore be impacted by how they frame situations. Under prospect theory however individuals may not necessarily be risk averse and risk attitudes are not a constant or fixed element of character and sometimes illogical or inconsistent choices can be made (Kahneman and Tversky, 2000). Levin et al., (1998) indicates a diversity of effects on framing which influence what is framed and how. This is significant because this accounts for factors other than simple rational choice to influence risk decision-making. Toyoda et al., (2007) provide empirical support for the theory in a study of financial risk decision-making among Japanese students which shows that this conceptualisation has high explanatory value.

A criticism of cognitive studies of risk relates to the experimental methods utilised which have been based on 'social settings' and has called into question their objectivity (Latour and Woolgar, 1986). The social setting of the studies requires them to demonstrate unequivocal objectivity and to account for social and cultural factors that need to be considered. For example, in gambling there is a 'gambling culture', choice may not be solely determined by rational consideration in such situations (Baumann, 2007). This suggests that social and cultural factors underpinning cognitive processes have yet to be taken into account generally, and also specifically in relation to awareness of risk.

Recent psychological research implies that risk awareness can be underpinned by other cognitive aspects. Kunda (1999) and Lee (2009) found that cognitive judgements can be positively or negatively influenced by factors including emotions, attitudes, and motivation which psychologists have termed "hot cognition".

2.3.2 Emotional Risk

In addition to rational processes, alternative theories suggest risk awareness and perception are impinged by emotions (Kahneman and Frederick, 2002). Lee (2009) highlights that negative emotions can compromise cognitive judgements implying that emotion can significantly influence risk decision-making processes. This highlights the importance of effective development of risk awareness to support cognitive decision-making. Epstein (1994) notes a dual-dimensional system of thought, often referred to as the analytic

(cognitive) dimension and the experiential (Epstein, 1994). Hogarth et al., (2010) describes the emotional dimension as covert activity of the experiential involving unidentified feelings and emotions, further suggesting that potential risk awareness can be driven by underlying emotional issues. For example emotions may inject bias in relation to how people perceive their environment. This is supported by evidence from Slovic et al., (2002) who demonstrated that judgements can be influenced by even modest levels of emotion such as day to day moods and affects which impact everyday decision-making and thinking. However, according to Slovic et al., (2002) emotions are often functional and rational in their use having emerged through evolutionary processes. This indicates scope for identifying key emotional dimensions which can factor into risk awareness.

Empirical research has significantly underlined the role of emotional factors in risk perception and awareness (Hogarth et al., 2010; Slovic and Peters, 2006). For example key findings by Lerner et al., (2003) highlight that negative emotions such as fear and anger can significantly influence risk awareness after a catastrophic event. Other studies using experimental methodologies have focused on the intentional manipulation of mood states to explore the influence on risk perceptions. Following this strand of research Rottenstreich and Hsee (2001) found that in circumstances where the consequences of uncertain actions involve either strong positive or negative affect, reactions generally lack recognition of wide variations in probability that the outcome will actually occur. Nevertheless scholars have emphasised that the theoretical conceptualisation of the link between risk and emotions has yet to be properly expanded and defined (Zinn, 2004; Wilkinson, 2001). For example conflicting findings have been found on the relative effects of emotional states on general and specific perceptions of risk (Johnson and Tversky 1983; DeSteno et al., 2000). This potentially has significant implications for the practical and organisational application of risk awareness as Zinn (2004) argues that risk management based on a narrow technical or statistical focus fails to capture the significant complexity that is inherent in socio-cultural and emotional factors. However Hogarth (2011) contends that limited knowledge exists in relation to how emotions and moods affect and contribute to daily risk perception and awareness.

An empirical study by Hogarth et al., (2011) studied the effect of everyday mood states and emotion on routine risk perception. Data was collected on three emotions of valence (pleasure), arousal, and dominance and found that wide differences in risk perception could

be explained by emotions and mood states. In particular more pleasurable mood states were associated with lower perceptions of risk which supports Hogarth et al., (2007). A notable finding showed that the emotions of valence and arousal accounted for variance to a greater degree than rational considerations, consistent with Slovic and Peters (2006) and other studies which have pointed to the importance of a shared role within risk perception for both rational thinking and emotions. The findings also showed that real-time judgements generally tended towards higher perceptions of risk than those made retrospectively when considering the same situation. The result hints at the dynamic and changing nature of the experiential cognitive system which according to Epstein (1994) is continuously adapting to perceptions of the environment.

The experimental methodology used in the study based on representative design principles is argued by Hogarth et al. (2011) to lead to meaningful and generalisable results in relation to the affect of daily mood states on risk perceptions. The study used an Experience Sampling Method to collect random samples of daily moods, emotions and behaviour from participants in conjunction with perceptions of current risks. The method is potentially highly appropriate for identifying immediate and direct linkage between emotions and risk awareness and overcomes the difficulty entailed within many studies of risk perception in relating findings to situational relevance. However Hogarth et al., (2011) highlight a significant study limitation in the inability to identify the directionality of causality within the analysis.

2.4 Behavioural Theory of Risk

2.4.1 Deterrence Theory

A notable unit of analysis within risk research is behaviour which Murray-Webster and Pellegrinelli (2010) argue is as a result of the potential for individuals´ cognitive biases to undermine the rational perception of risk and influence decision-making. Anticipating risk behaviour forms the basis for the general deterrence theory which seeks to explain the effectiveness of organisational security countermeasures. The theory´s significance for the study objectives lies in its potential explanatory power and widespread utilisation within industry practice to reduce systems risk as the first phase of a general security cycle continuing with prevention, detection and recovery (Forcht 1994; Straub and Welke 1998). The deterrence phase focuses on influencing individual behaviour and aims to prevent the

intention to commit anti-social acts through the administration of strong sanctions and disincentives. Deterrence theory holds that when the effectiveness of the security system is evident to a potential systems abuser in terms of the severity of punishment and its certainty, the rate of committing abuses reduces. This is termed the deterrence feedback loop and its function is to strengthen the proposition that potential abusers become aware of the consequences of their actions (Straub and Welke, 1998). The relevance of the deterrence theory to risk awareness relates to the fact that at least 50% and up to 75% of systems misuse is by internal users (Hopkins, 2013). In line with this, Darcy et al (2008) found that users´ awareness of their behaviour in respect of gains and impacts through risk awareness and education and training reduced IT misuse. Their research established a direct relationship between user awareness of security countermeasures and the organisational sanctions associated with instances of IS misuse, with knowledge reducing cases of IS misuse and possible misuse intentions. This is supported by earlier research focusing on applied general deterrence theory within the IS environment which found that systems risk can be reduced by appropriate security actions (Straub et al., 1994; Straub and Nance, 1990). An extended deterrence model was tested on 269 computers from 8 different companies and notably identified that user awareness of security policies was among three main practices which effectively deterred IS misuse.

However, despite broad implementation within many organisational risk management strategies empirical evidence supporting the theory is inconclusive. A study by Wiant (2003) of 140 IS managers indicated that the nature of organisational security policies had no direct or indirect bearing on the severity or quantity of security-related incidents. Further Foltz (2000) found that usage policies within a university IT system had no conclusive impact on system misuse intentions and behaviors including stealing, modification and destruction of either software or data. This suggests that further research is needed to understand and explore the different facets and dimensions of deterrence practices which may have an impact on risk-taking behaviour.

Notably these studies relate to different industries and contexts which imply that deterrence theory and its impact on risk awareness can vary. D´Arcy et al., (2008) provide an indication of the multi-dimensional nature of deterrence as their results show that in the IT context perceived severity of sanctions had a stronger deterrent effect than perceived certainty. Notably the results differ from criminological and sociological studies yet accord with earlier

work in the IS field. This also underlines the different influences of contextual factors on risk awareness and deterrent influence over behaviour.

Young (2010) invoked general deterrence theory to study the impact of formalised information security on collaborative exchange. As the basis for risk awareness this work established practicable application of formal communication channels for information security policy-making and enhancement of understanding of detection, deterrence and recovery activities. Though behavioural deterrence theory is significant for understanding risk awareness, there are no significant studies that use deterrence theory as the focal theory and which result in remarkable contribution to understanding risk awareness.

Murray-Webster and Pellegrinelli (2010) contend that risk management theories and best practices fail to take account of practitioners´ intuitive and personally-driven behaviour in relation to managing risk and uncertainty. In particular, it is asserted that risk management planning tends to emphasise proactive mitigation of risks and threat reduction while ignoring contingent actions and the generation of options which Benaroch et al., (2006) shows is more closely aligned with the intuitive option-based logic of risk managers. In today's diverse and dynamic IT context the intuition of a wide range of stakeholders is arguably vital in developing a wide base of risk awareness. A disconnect between risk strategies and the experiences and knowledge of individuals suggests a lack of theoretical and practical understanding of behaviour in this respect.

Reconciling economic rationality with these behavioural tendencies in risk management practices, Murrary-Webster and Pellegrinelli (2010) controversially argue that "the focus should be on adding economic value rather than reducing risk per se" in business projects. They assert that opportunity gain/loss is a better metric for gauging potential impacts on risk events and that "creation of real options should be emphasised as part of the repertoire of generic response actions to risk." (p. 1). Nevertheless the study is not empirically based and further research is required to explore actual behaviour and the relationship with theory and practice.

2.4.2 Risk Homeostasis

The homeostasis theory of risk in social science is essentially a risk management theory describing a condition wherein individuals, organisations and societies develop an inherent level of risk which they are prepared to accept and manage (Shomack and Stewart, 2008). In relation to IT security homeostasis has the potential to undermine measures designed to counter threat. The theory originates in the risk compensation theory and target risk concepts of Peltzman (1975) and Wilde (1994) focused on user behaviour within the transport sector. It is asserted that despite efforts to remove or mitigate accepted risk in one area users will increase risky behaviour in another to compensate thereby maintaining a risk perception balance. Wilde (1994) refers to this attitude as 'target risk', which is the risk individuals and societies are willing to accept in their subconscious mind. These other risks are blindly accepted or non-cognisable. This suggests that within the information security risk structure any system implemented to reduce security risk in one aspect will result in an increase in security risk in other aspects. Empirical evidence by Pattinson and Anderson (2004) in relation to information security found that behavioural factors potentially including risk homeostasis were significant for formulating risk management strategies.

The notion of regulating risk by reallocation known as risk homeostasis is significant because it implies the limitations of rational approaches. It is not possible to calculate risk comprehensively or to address it without understanding the subjective view of individuals within the organisation. However it should be noted that there is limited theoretical reason for accepting the risk homeostasis hypothesis as according to Haight (1986, p. 364), the incoherent "theoretical formulation" of risk homeostasis is the reason why the concept attracts arguments disproving its validity. In a long-term longitudinal study of driving behaviour following the introduction of safety laws and measures Robertson (1998) finds no empirical support for risk homeostasis. Robertson and Pless (2002) argue that risk homeostatis is improbable as people do not have enough knowledge, attention or ability to adjust their risk taking behaviour to maintain constancy. The affect of awareness is not clear and according to Shostack and Stewart (2008) user awareness training measures to address homeostasis have proved inconclusive. This theory suggests that different individuals will have different perceptions of what level of risk is potentially acceptable or probable in their context. Awareness may play a role in this regard and while there is lack of evidence of user

awareness training to address this (Shostack and Stewart, 2008) other more experiential methods to enhance awareness may impact on the calculation of risk.

2.5 Sociological and Cultural Theory of Risk

Sociological streams of research have also examined risk from a number of perspectives including cultural. Whilst the cognitive and behavioural units of analysis of risk have improved understanding of risk and risk management, they are limited to individuals. For enterprise risk management, the sociological and cultural unit of analysis are relevant units of analysis because they reflect complex interrelationship elements such as norms, values and rituals which have a far reaching influence on behaviour (Mullins, 2010). Consequently sociological and cultural factors can influence individuals' awareness of risk.

The importance of context and culture in risk awareness has been underlined by theorists who have proposed that organisational culture can also impinge on risk perceptions (Karyda et al., 2004). Schein (1984) developed a model of risk culture of enterprises composed of three elements: basic assumptions, values, and artefacts and creations. Basic assumptions include employees' perceptions, thoughts, and feelings about risk, which shape a company's risk culture. Basic assumptions are the intangible aspects of organisational and environmental relations that are commonly taken for granted. Values determine employees' moral and behavioural standards. Such values in turn determine their principles, taboos and unwritten guidelines and these values are only partially visible from their behaviour. Artefacts and creations are tangible, such as the risk manual and guidelines, risk managers, and risk management committee. These artefacts and creations whether they exist or not enable managers to assess the existing risk culture of the enterprise (Schein, 1984).

Cultural theory has become a significant conceptual perspective for the examination of risk perceptions and interpretations (Wildavsky and Dake, 1990) and seeks to explain the manner in which people perceive and act in their environment. Douglas (1978) advances that people tend to subscribe to one of four worldviews identified as egalitarian, individualistic, hierarchical and fatalistic depending on the social environment to which they belong with practical implications for risk management strategies. Egalitarians for example tend to be sceptical of expert knowledge in contrast to hierarchists who further accept risk measures as long as they are justified by authorities (Oltedal et al., 2004). This may suggest a barrier to risk awareness if communications from such sources are filtered or discounted.

However empirical studies show mixed support for the theory. On the one hand Wildavsky and Dake (1990) show that cultural adherence to worldviews is a significant predictor of perceptions. In the study the latter was shown to have the highest predictive power which it was claimed provided significant support for cultural theory. This was not supported however by other studies including a qualitative study of the risk perceptions of UK residents by Marris et al., (1998) which found more support for psychometric explanations of variances in risk perception than cultural differences.

The result is further consistent with Sjoberg (1996, 1997) who also found that psychometric models more accurately explained risk perceptions than cultural theory. In a study which compared risk perceptions between Swedish and Brazilian samples findings showed that the relationship between cultural adherence and risk perceptions were low with both groups judging risks in similar ways. Sjoberg (1997) argues that the findings indicate that risk perception is more greatly linked to real risks than cultural values and assumptions and further that an individual´s risk attitude has much higher explanatory power than cultural theory.

It is possible that the lack of empirical support for the theory may have emerged as a result of inadequate operationalisation within existing research. For example Oltedel et al., (2004) highlight that the methodology utilised by Wildavsky and Dake (1990) to empirically support cultural theory was limited by a restricted number of measures to test cultural adherence which challenges the ability to encapsulate the differences in worldviews and separate them in terms of risk perception. Moreover the ability of cultural theory methodologies to explain risk perceptions and attitudes is challenged by an individual´s ability to conform to more than one worldview in different contexts. Consistent with Sjoberg (1995), Marris et al., (1998) found that a significant proportion of the sample did not adhere solely to one worldview. This suggests that cultural adherence is not an innate individual trait which can be captured and identified by means of a questionnaire designed to reflect a single worldview and can be influenced by the context of the individual who can potentially be hierarchists at home and egalitarians at work. Tsohou (2014) highlights that this potential supports a mobility view of cultural theory in which individuals may often link with social structures with differing cultural biases in varying areas of their lives, suggesting that people may adopt various cultural biases according to context and over time. Therefore it is asserted that cultural bias

cannot be measured separate to specific contexts and timeframes implying a qualitative approach to evaluation. Nevertheless Tsohou (2014) highlight the lack of empirical research and practical development of risk management models which emphasise comprehension and management of the perceptions of IS stakeholders. Oltedel et al., (2004) highlight that the extent of differences between individuals potentially implies that the acceptance of an overall cultural theory is naive and misguided.

A risk culture however is significant for managing organisational risk because it impacts on employees' awareness of IT systems risk. Through such awareness they recognise the structures and processes for managing risk and begin to support them by changing their behaviour. Arguably, peoples' awareness of risk is a combination of cognition, behaviour and the social and cultural setting.

2.5.1 Systems Theory and Socio-technical Systems

Systems theory engages in a holistic view of objects in which the fundamental purpose is to make each individual part perform optimally without interfering with the whole system (Winter and Checkland, 2003). Systems theory is applied to understand technology organisation in a social setting (Checkland, 1981), organisational data, information and knowledge and management (Emery and Trist et al., 1965; Horlick-Jones, 2007).

A distinction between hard and soft systems is drawn by Winter and Checkland (2003). In the 'hard system' approach, a situation is characterised by its environment and surrounding clarity on the basis of which goals are established through core planning activities and implemented, maintaining firm control. Many existing risk management systems are based on perceiving risk utilising a 'hard system' perspective. In the 'soft system' approach, a situation is characterised through its uncertain, complex and dynamic positions. This approach focuses less on management processes and rather on managing situations through understanding of how managers perceive and evaluate phenomena, and how they decide to act, which itself becomes a part of the dynamic situation (Winter and Checkland, 2003). The approach is potentially effective in taking into account the emotional and behavioural dimensions of risk and risk awareness which appear to be neglected in harder systems approaches.

Socio-technical systems theorists characterise organisations as 'open technical systems', which both influence and respond to the wider environment (Emery and Trist, 1965). Since information systems are composed of people, IT and organisations, they can be characterised as socio-technical systems (Hevner et al., 2004). By considering each of the components as interdependent it provides better understanding of IS development. An empirical study by Al-Fehaid (2003) into risk of adopting IT-based accounting systems found that adoption resulted in 'possible increase in audit risk' which was related to "lack of understanding" by client's management. While these results emphasise the impact of socio-technical dimensions on risk awareness there is a notable gap in the literature on this topic.

2.6 Risk Management

The description of risk management in the literature suggests the identification of risk, and the assessment of risk and control of risk (Borodzicz, 2005; Chapman and Ward, 2002), as shown in Figure 1.

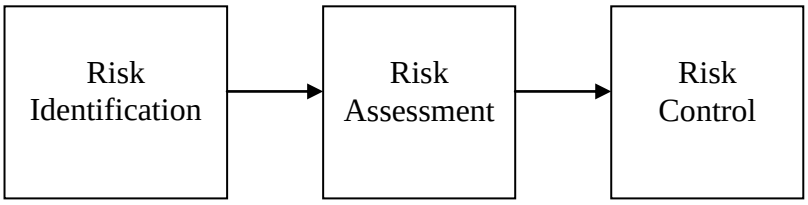

Figure 1 Risk Management Process

Risk identification is the first stage of risk management. It identifies the nature of the risk, the areas where risk may emerge and monitors the potential threats which affect the enterprise or organisation. Awareness of critical risks and their definition occurs at this stage. Risk assessment can then be undertaken against a set of regulations or rules that the company is adopting for that particular industry. Such assessment is necessary to ensure compliance with legal requirements and other professional and ethical standards. This aspect implies a high level of awareness of compliance in IT prior to initial assessment. This is a major challenge given the rapidly changing IT context outlined earlier. At this stage all risks that have been identified in the first stage must be revealed and scaled against the regulations in this stage. However IT risks emerging from cyber-crime, cloud computing, data protection and disparities in regulations across different regions emphasise the challenge in ensuring that individuals have sufficient level of awareness to undertake risk identification and assessment effectively. This extends to the third stage of risk control. Chapman and Ward (2002)

explain that the process of managing implementation of risk procedures involves on-going monitoring and controlling of the project by taking into consideration the implications of the risk management procedure. An awareness of appropriate measures and solutions underpins the effectiveness of risk control.

The process of risk identification and assessment however is a highly subjective and complex process. The classification of the literature on risk management in the above sub-sections is different from that presented by Ikram's (2000) study of risk management in IS. Ikram used the epistemological and ontological dimensions used by Burrell and Morgan (1979) as two categorical scales. The scales are Regulation to Change and Objective to Subjective. This analysis results in four 'paradigms' of sociological inquiry: functionalist, social relativist, radical structuralism and radical humanist. Ikram (2000) then classifies risk and studies of risk in terms of these four paradigms.

In the functionalist paradigm, risk is assumed to exist independent of the observer and that risk can be objectively measured. This "assumes that risk and its consequences can be measured by empirical observation, since the causal agents that are responsible for negative effects would remain stable over the predicted time period" (Ikram 2000, p.18). In the social relativist paradigm risk is socially defined and constructed. Peoples' values and perceptions determine what is undesirable. "The perception of risk changes through continuous social learning, therefore, risks and their manifestations are social artefacts fabricated by social groups or institutions" (Ikram 2000, p.18). Radical structuralists believe the social world has the same objective composition as the physical world. The level of risk is perceived as existing independently of the observer and that it is real, and therefore it can be objectively measured using scientific methods. They assume that "the level of risk cannot be understood without a prior analysis of the social structures within which risk is thought to exist. The focus therefore is on the normative aspect of emancipation, which can be viewed as empowering groups to be able to determine their own acceptable level of risk" (Ikram, 2000 p.19). Radical humanism believes that risk is socially defined by groups and institutions and that it is a social artefact. Risk does not exist independently of the observer. "It seeks an emancipator discourse about defining risk that facilitates the widest possible debate and within which one must acknowledge the other person as a partner in human interaction" (Ikram, 2000 p.20).

Using Ikram's (2000) classification of risk, the present research would be classified as social relativist. IT systems risk awareness is socially defined by risk strategists and managers with their co-workers. The determination of what constitutes threats and attacks on IT systems is by risk strategists and managers. Significantly, as Ikram (2000) argues the perception of risk is constantly changing and being reconstituted by the social group as they continuously learn about risk. Ikram (2000, pg.23) argues that there are three characteristics of risk in IS, an undesirable consequence, uncertainty and "possibility to affect the risk through conscious change". This characterisation of risk serves the aim of the present research well, since it aims to measure risk and thereby affect change in IT risk awareness.

In contrast to Ikram's (2000) epistemological and ontological classification, other risk studies in IS focus on specific risk factors. Enterprise resource planning systems (ERP) play a significant operational role in organisations, covering core business processes as well as management and support processes. Currently ERP systems extend beyond the organisation in supply chain management. Eurich et el.'s (2010) research shows that the willingness of companies to share item-level data in supply chains is constrained by perceived privacy risks. Based on their study, they propose 'inter-organisational data sharing infrastructures" as a solution to the problem of sharing. They identified seven risks that prevent organisations from sharing data, including reconstructing strategic decisions, threat to be penalised for unfair behaviour and loss of information advantage. Drawing on the findings of their study, they propose that data sharing can be increased by: (a) devising fine grained access control system; (b) methods related to secure multi-party computation, and (c) every party sharing data with a trusted third party.

Risk management can be defined as the determination of potential dangers and problems, the evaluation of their significance and the investment in planning to monitor and manage those issues should they arise (Hughes and Cotterell, 2002). Verbano and Venturini (2013) define risk management as a process which is designed to protect company assets against losses which may impinge on current gaps. The adoption of risk management can provide greater certainty in enterprise management to ensure continuity of trade and production and can reduce the risk of failure while promoting organisational image both internally and externally (Verbano and Venturini, (2013). Risk management therefore supports the creation of business value through maximising profits while minimising costs (Urciuoli and Crenca, 1989).

Within the practice of information system risk management the main objectives are the identification of security risks, prioritisation, determination of the most effective method for controlling security risks such as avoidance or mitigation and the monitoring of changes within the risk management system. Critical to the process is an effective assessment of the overall situation in terms of risk involving significant information collection in relation to IS resources. However evidence shows that IS risk management as is commonly practiced within organisations is potentially highly ineffective. Evidence shows that often the process is conducted infrequently and sometimes only when perceived as needed in place of a routine schedule (Rees and Allen, 2008). This further compounds problems within risk assessment as infrequent performance means that vast amounts of information need to be gathered and analysed over a short time scale (Webb et al., 2014) and can present only a snapshot of the organisation´s status despite the dynamic information environment within which contemporary organisations operate (Schmittling, 2010).

Studies have also shown significant flaws in risk assessment practices. Notably Matwyshyn (2009) provides robust evidence that organisational approaches to IS risk management can tend towards a tick-box compliance mentality in which the need to increase information security is reasoned away through the consideration that formal compliance with legal boundaries is sufficient assurance. Moreover a range of studies have highlighted significant deficiencies in risk identification and assessment with major sources of risk commonly omitted (Parker, 2007; Utin et al., 2008; Shedden et al., 2011). Shedden et al., (2011) indicate that risks related to intangible knowledge assets such as distributed tacit knowledge are routinely ignored while Utin et al., (2008) shows the common failure to determine risks associated with the complex relationships between diverse information assets. Furthermore information security risks are often assessed with limited relation to the actual situation of the organisation (Webb et al., 2014).

This points to significant shortcomings within the common practice of IS risk management particularly in the area of risk analysis. Baskerville (1991) however highlights that often risk assessment lacks foundation in concrete evidence, and key data values such as risk probabilities and loss estimates are commonly highly interpretative with little systematic investigation. More recently, Parker (2007) emphasises that both quantitative and qualitative approaches to risk assessment are highly simplistic. This view is supported by Udin et al,

(2008) who further points to the conventional impossibility of including all the many relevant risk variables such as users, computer and business environments.

Nevertheless a search of the available research databases found few studies on IS risk management, even though it is widely acknowledged that IT systems are central to organisations´ operations. Information systems researchers tend to focus on how to develop IS. The research methods used for these kinds of studies include case studies, quantitative survey analysis and examples of action research.

2.7 Enterprise Risk Management

Enterprise risk management (ERM) is a wide-ranging and complex concept that encompasses all key areas of an organisation. Hampton (2014) defines ERM as:

"the process of identifying major risks that confront an organization, forecasting the significance of those risks in business processes, addressing the risks in a systematic and coordinated plan, implementing the plan, and holding key individuals responsible for managing critical risks within the scope of their responsibilities" (p.20).

Definitions of ERM address this concept at three levels of strategic, functional and process (Hampton, 2014). This in turns implies different levels of risk awareness in relation in IT contexts. At the strategic level a focus on risks impacting on results is important, while at the functional level the focus shifts to risk associated with activities. At the process level risk awareness may be concerned with actions to manage risk.

COSO (2004) states that ERM is "a process, affected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".

This emphasises the integrated nature of risk within ERM. Consequently this broadens the conceptualisation of risk awareness in a way that reflects a dependency on events beyond individual immediate context. It is suggested that while risk management can be a highly specialised process research has found that organisations function more effectively when all

members are involved in the risk management process (Stoney, 2007; Power, 2004). ERM is a holistic, enterprise-wide approach to managing risks and centralising risk information (Alviunessen and Jankensgård, 2009) and implies that all types of risks are integrated or aggregated in risk analysis, and integrated tools and techniques are used to communicate across business unit boundaries (Ahmed and Tahir, 2011). ERM approaches are therefore systematic and integrated which negates the management of risks in departmental silos and assists in identifying risk appetite (Ahmed and Tahir, 2011). This further ensures that risks are mitigated or avoided in alignment with risk tolerance and firm objectives (Walker et al., 2003). These points underline the significance of risk awareness measurement to reflect an enterprise-wide perspective at various levels.

The COSO framework has four categories of objectives to help enterprises meet their goals: (a) Strategic – high-level goals, (b) Operation – effective and efficient use of resources, (c) Reporting – reliability of reporting and (d) Compliance – compliance with applicable laws and regulations. The eight components of the COSO framework provide a comprehensive coverage of enterprise-wide risk management and reflect a range of sub-components which are underpinned by risk awareness.

There is substantial consensus in the literature that a Risk Management framework should contain some method for risk identification, risk modelling, risk assessment, risk control and risk management (Hillson, 2006; Border, 2000; Graham and Kaye, 2006; Hancock, 2001; Rashid and Allan, 2005;Haimes, 1998; Simon, 1997; Ansell and Wharton, 1992; Coyle, 2002; Vasarchelyi, 2002). Other authorities agree that risk management contains eight steps for risk: define, focus the process, identify the issues, structure the issues, clarify ownership, estimate sources of variability, evaluate overall implications and manage implementation (Chapman and Word, 2002). Within ERM frameworks the importance of risk awareness has been highlighted. For example Bayaga and Moyo (2009) assert that in order for organisations to enable enterprise-wide risk responsiveness and preparedness all organisational members need to have knowledge and understanding of organisational risks. The findings of their study into risk awareness in the context of university ERM shows that risk awareness is associated with organisational risk preparedness, through the understanding and documentation of risk policies and procedures and the formulation of a risk treatment plan (Bayaga and Moyo, 2009).

2.8 IT Risk Management

The pervasiveness of IT into every aspect of society underlines the significance of IT risk management. The myriad risks associated with technology and digital technologies have profound repercussions for all areas of society. However, the study of IT systems risk is a relatively recent development. In spite of a number of conceptual studies, few have any empirical basis.

Risk in the IT context has frequently focused on specific risks relating to viruses, password cracking, and firewall penetration. Goodue and Straub's (1991) study states that IT security is a function of inherent industry risk, measures of effort made to control those risks, and individual factors like awareness of prior attacks and previous experience. Their proposed model addresses the role of awareness in risk defining managerial perceptions of security risk based across three variables: organisational environment and beliefs about industry susceptibility to industry risk; IS environment and actions to effectively secure systems; individual characteristics, and awareness/knowledge of systems and local systems risk. Independent verification of these factors has been reported by Dixon et al. (1992). These studies clearly indicate 'awareness' as an issue in IT systems risk management.

Pember (1996) recognised that risk managers needed to be "very aware of the potential risks" (p. 36). Her investigation resulted in a model of risk management for IT detailing five components: (a) Acceptance of risk and mandate from top management, (b) Identification and assessment of risk and development of worst case scenarios, (c) Elimination or minimisation of potential risks, (d) Creation of formal disaster recovery plan/s and (e) Transfer of risk.

The National Institute of Standards and Technology (NIST) in the U.S provides a methodology for IT risk management (Stoneburner et al., 2002). It defines risk as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation" (p.8). It asserts that "the risk management process is on-going and evolving" (p.41) as computer networks and Internet networking is continually expanded and updated, its components changed, and its software applications replaced or updated with newer versions. It thus proposed 'on-going risk evaluation and assessment' using its methodology. In the NIST methodology risk

management is conducted and integrated based on the Systems Development Life Cycle (SDLC). It requires a specific schedule for assessing and mitigating 'mission risks' but advocates flexibility to respond to major changes to IT systems. The key success factors for implementing the methodology are: "(1) senior management's commitment; (2) the full support and participation of the IT team; (3) the competence of the risk assessment team, with expertise to apply the risk assessment methodology to a specific site and systems, identify mission risks, and provide cost-effective safeguards that meet the needs of the organisation; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the missions of their organisation; and (5) an on-going evaluation and assessment of the IT-related mission risks." (p.41). In addressing 'the awareness and cooperation of members' the NIST methodology marginally explores the issue of risk awareness and fails to provide any conceptualisation of components or measures of risk awareness.

2.9 Numerical and Statistical Models of Risk

Quantitative-based models of risk emphasise the role of numerical and statistical analysis in risk management. Mathematical and statistical models of risk too seek to understand the nature of risk, and these quantitative models are the cornerstone of the other applications of risk (Guehlstorf, 2004). They differ from causal theoretical explanations because, additionally, they uncover the mechanisms of risk and specifically how risk can be measured and calculated (Makowski, 2005).

It has been seen that other mathematical and statistical models for risk analysis are available (Vose, 2008). Simplistic risk analysis models consist of 'What if' scenarios, usually involving the use of basic spreadsheets. Quantitative risk analysis (QRA) is a more comprehensive and in-depth approach which evaluates every single value for each variable and adds weights to reflect the probability of its occurrence (Vose, 2008). The basic deterministic model is usually constructed on a spreadsheet used to undertake what-if analysis. Influence diagrams can be used to represent variables as nodes and the connections between them as arcs. With complex risk problems influence diagrams become unwieldy. Event trees are descriptive risk analysis models. They map the probabilities of a sequence of events and calculate the probability of the sequence (IET, 2012).

Risk assessment can also be based on probabilistic models which have been increasingly employed within information security analyses. Probabilistic methods have been found to be effective for providing the basis to make informed resource deployment choices which maximise resource use thus enabling increased risk mitigation and cost savings (Ostrom and Wilhelmson, 2012).

The Monte Carlo Simulation is a further risk assessment method which utilises mathematical algorithms to solve problems which cannot be analytically resolved (Hayes, 2011). This has been widely employed within risk assessment and significantly utilised across a wide range of disciplines to model risk. There is a debate regarding the effectiveness of this method however. Monte Carlo Simulation has the advantage of being able to be used in complex statistical inference problems and can be refined across two stages for greater accuracy. Nevertheless Ferson and Ginzburg (1995) emphasise that this model has a high requirement for information which must be supplied either through data or assumptions. Moreover it is argued that on the occasion that assumptions or imperfect information is used model outcomes can be over-precise. Nauta (2000) further argues that the amalgamation of sources of knowledge uncertainty such as subjective judgements, variability or measurement error into one single density function can lead to potentially confused or erroneous results.

Discrete event simulation (DES) is an analysis tool derived from systems theory and models the behaviour of a system over time (Banks et al., 2005). DES can be used to model the impact of certain decisions. For instance what would happen in the event of a terrorist strike on government IT systems or a major hack of enterprise IT systems. A DES can be set up with the known entities and the range of values added or run to see what would happen. A significant advantage of DES for risk analysis is the capability to model complex risk scenarios and the dynamic dimensions and changes within systems and situations (Markert and Kozine, 2012).

However limited research exists in relation to risk analysis in the field of information systems. One study by Herrmann (2013) involved 36 participants to execute an experiment related to risk estimation. The purpose of the participants was to estimate IT-related risk probabilities while the researchers investigated the IT-related risks on the basis of various risk estimation factors: computing experience, age of the estimator and other factors. The findings notably showed the difficulty for users in estimating risk probabilities and further

that these probabilities can be over-estimated to the extent of seven hundred percent. The findings also indicated the challenge in estimating low risk probabilities. The limited evidence points to the importance of understanding the variations and tendencies within users´ estimation of risk which may impact and undermine the effectiveness of risk awareness strategies.

Risk assessment can further employ non-probabilistic models. Possibility theory based on the utilisation of fuzzy sets is a non-probabilistic risk analysis model. A central concept of fuzzy sets is the idea of relation and membership which clarifies the existence or otherwise of association (Hayes, 2011). Fuzzy sets function through the manipulation of non-probabilistic uncertainty to represent imprecise or incomplete information (Matta et al., 2012). An alternative non-probabilistic model for risk assessment is interval analysis which is one of the most straightforward and basic methods to manage knowledge uncertainty and variability when assessing risk (Hayes, 2011). The method functions utilising deterministic and conservative methodologies to assess risk based on finding the worst and best case. However this method has significant disadvantages in the tendency to result in extremely conservative risk estimates and arbitrary protection standards (Burgman, 2005). Moreover, risk estimation can be influenced by the degree of risk awareness of individuals.

2.10 Conclusion

This chapter has reviewed literature on the general notion of risk and risk management and a number of underlying psychological, behavioural, sociological and rational theories. The literature identifies several theories and perspectives on risk and risk management. The theories emphasise complexity and subjectivity of risk identification and assessment both qualitatively and quantitatively. While the literature reviewed has identified that risk awareness either has an impact or underpins risk management there is gap in its´ conceptualisation.

The survey of risk management literature suggests that risk awareness is not understood or addressed by most organisations. While the orientation of IT management emphasises socio-technical dimensions they fall short for instance in the case of the NIST model in explaining risk awareness. One central reason for choosing to develop a model of IT systems risk awareness is to improve the generalised outcome of the present research. Since these models are abstractions of empirically observed phenomenon, they are more generalised. The reason

for proposing the generic risk management process model above is to support the abstraction process. The generic model informs the development of the conceptual framework in the following chapter that forms the basis for developing the conceptual model of IT risk awareness.

Chapter 3: Conceptualisation of Risk Awareness

3.1 Introduction

This chapter presents a review of IS and IT risk management literature on the topic of risk awareness and specifically IT systems risk awareness. This review provides critical insights and understanding into conceptualising risk awareness and identifies key findings and gaps in the literature on this topic. This begins with the concept of risk awareness and iteration of its importance to IT risk management. Several general approaches and related studies are reviewed followed a discussion of specific dimensions of risk awareness identified in the literature.

3.2 Concept of Risk Awareness

Risk awareness is defined as an individual's perception of and compliance with risk management policy and procedures. Awareness is knowledge or perception of a situation or fact (Oxford Dictionary, 2013). It is the cognitive state of 'knowingness'. Since it is individuals or organisational employees who enact business processes involving IT systems, the effectiveness of IT risk management in organisations depends on individuals' awareness of IT risk. Risk awareness is also defined in relation to the degree of convergence between what is perceived as the danger of the task and the actual reality of the danger. Therefore a greater level of convergence leads to increased quality of risk awareness (SWOV, 2010).

However the literature has noted the lack of conceptualisation of risk awareness. Siponen (2000) argues that approaches to 'information security awareness' are descriptive, that they are "not accomplishment-oriented nor do they recognise the factual/normative dualism; and current research has not explored the possibilities offered by motivation/behavioural theories." (p.31). To fill the gap he constructs "a conceptual foundation for information systems/organisational security awareness", and using the behavioural science framework consisting of intrinsic motivation, a theory of planned behaviour and a technology acceptance model, provides a novel persuasion strategy "aimed at increasing users' commitment to security guidelines". This work has direct relevance to the present study of user risk awareness in that it takes people as the unit of analysis. The theoretical framework is aimed at 'increasing users' commitment to security guidelines' but it does not provide specific measures to gauge whether increased awareness has occurred.

The individual reflective aspect of risk management is emphasised though the notion of human awareness in terms of the ability of people to recognise their own experience and also that of others. In addition to that, people monitor events in their own lives and make decisions for the future based on their knowledge and then communicate this awareness with others. This is termed awareness of the self and awareness of the other people (Markova, 1987). As noted earlier in the Section on theories of risk, culture is important. Cultural awareness is the term used to describe behaviour on language use and communication (Tomalin & Stempleski, 1993).

Straub and Welke (1992) empirically research two propositions. One, "Managers are aware of only a fraction of the full spectrum of actions that can be taken to reduce systems risk" (p.447). Risk awareness is increasingly vital to understanding and avoiding risky situations and a fundamental component of the effective management of risk. There is a growing consensus in industry however that the concept of risk awareness is an issue which requires significant attention. Today, the role of risk awareness and its importance within an enterprise is widely recognised among the wide ranging types of enterprises; large, small, profit- and non-profit making, service and manufacturing businesses and government organisations. According to a report in Continuity Central website (ContinuityCentral.com, 2012), research conducted by Aon (2009) revealed that: "70% of UK risk managers have declared that making sure the employees in their organisation are 'risk savvy' is their biggest challenge". The risks faced by companies have increased dramatically in a range of categories and the number of incidents such that it is considered significant enough that they "... need to be dealt with by employees throughout the organisation..." and not just by senior managers alone.

3.3 IT Risk Awareness

IT risk awareness is a common theme in the literature reviewed in the preceding sections. A key success factor for successful IT risk management noted by Stoneburner et al., (2002) is "the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the missions of their organisations" (p.41). Siponen (2000) proposes theoretically informed methods for increasing individual's IT risk awareness. Overall risk awareness however is the culmination of the combined knowledge of all members within the organisation.

Earlier studies reported that managers are '"naive" about the challenges posed by IT threats (Loch et al., 1992, p.183). D'Arcy, Hovav, Galletta., (2009) report that 50%-75% of IS security incidents originate from within an organisation. The situation has not improved significantly in the last decade. The CSI Computer Crime and Security Survey (2011) reports that 45% of respondents had been the subjects of at least one targeted attack. Similarly, in the PriceWaterhouseCooper (2010) survey, 92% of large company respondents had a security incident in the previous year and the median number of breaches was 45. The average cost of a large respondent's worst incident of the year was between £280,000 and £690,000. The incidence of staff leaking or losing data was 45%.

IT risk awareness is crucial because individuals in organisations may misuse, misinterpret or not comply with risk management policy, procedures and guidelines (Hoffer and Straub, 1989; Goodhue and Straub, 1989; Ceraolo, 1996; Straub and Welke, 1998). Effort placed on planning and implementing risk management strategies and setting up risk policies and procedures may not be effective when individuals' awareness of risk is either absent or inappropriate. Research has focused on understanding risk awareness and how to increase individuals' risk awareness to improve risk management implementation. However, risk awareness applies not only to managers, but also their subordinates and contractors.

Risk awareness is important to companies and their personnel. An effective level of risk awareness means that all concerned become clear of what threats prevail, how to recognise the early signs, what course of action to take to prevent it escalating and what action to take if the worst happens. It is also necessary for staff members within an organisation to clearly understand that certain actions taken by themselves (whether knowingly or inadvertently) may expose the organisation to serious unnecessary risks. It should also be clear that disciplinary action will be initiated against staff member/s, thus inducing some level of self-control and responsibility concerning deeds and actions permissible among the staff members themselves.

Kutsch (2005) argued that the lack of risk awareness by IT project managers would have an adverse influence on the outcome of IT projects. It is suggested that in order to prevent risks from adversely influencing the project outcome, IT projects managers should plan early to prevent risk related interventions from influencing the use of project risk management.

Notably, this study focuses on the timing of risk assessment by project managers rather than risk awareness more generally.

3.4 Approaches to IT Risk Awareness

Sipponen (2000) identifies two categories of research on IT systems risk awareness as 'framework' and 'content'. The framework category describes research that seeks to engineer IT systems risk awareness by creating awareness structures and developing quantitative measures, and it is formalised as explicit knowledge. Such knowledge can then be applied to improve IT systems risk awareness. The content category is "a more informal interdisciplinary field of study" (p. 31). He then mistakenly draws a parallel distinction between quantitative research methods as suitable for the framework category and qualitative research methods for the content category. This methodological dichotomy is mistaken as the researchers he cites, for example Straub and Welke (1998), have used qualitative research methods to construct 'framework' type research. This categorisation of framework and content is not useful for understanding IT risk awareness because it recasts existing distinctions and erroneously.

In research informed by the general deterrence theory, D'Arcy et al., (2009) investigated IT systems user awareness of security countermeasures or deterrence and its impact on IS misuse.. The findings highlighted that user awareness of security policies, security education, training and awareness (SETA) programs and computer monitoring deterred IS misuse by employees. Individual countermeasures were found to be effective to varying degrees in increasing perceptions of sanctions associated with IS misuse.

A project focused approached formed the basis of research by Kutsch (2005). It was suggested that IT project risk management processes are perceived by project managers as ineffective in minimising the risk to project outcomes. He studied the gap between how risk should be managed and how they are actually managed by project managers. Among other factors, Kutch's (2005) study indicates project managers' risk awareness to be a prime factor in the use of project risk management; "IT project managers were unaware of risks and considered them to be outside their scope of influence, and IT project managers preferred to let risks resolve themselves rather than proactively engaging with them." (p.ii). Therefore, risk awareness is a significant people issue in risk management. It is worth emphasising

managers' unawareness of risk and tendency towards inactivity in dealing with known risk. Creation of a holistic conceptualisation of risk awareness to underpin evaluation of risk awareness, the aim the present research, could help in addressing both issues.

The consensus shows that IT requires the implementation of project risk management to prevent loss or damage of data (Boeham, 1991; Royer, 2000; NIST, 2002; Allan, 2007). lkram (2000) concluded that "project managers take the view that organizational factors very often cause problems for the success of the IS development process." (p. 241), implying that risk awareness is a critical factor in risk management. Al-Fehaid (2003) concluded that "the increase utility of IT-based accounting systems and identifying the variables that are related to audit risk in Saudi Arabia." (p. 1-358). This work emphasises that more factors should be taken into account to help enhance the management of the risk in any organisation and that managers need to be aware of these.

Kutsch (2005) suggested that "the underlying rational assumptions of project risk management and the usefulness of best practice project risk management standards as a whole need to be questioned because of the occurrence of interventions such as the lack of information." (p. 1-255). A knowledge focus is also emphasied by Al-Shehab (2007) in a study which focused on defining desirable elements in relation to understanding of risk. The proposed model examined causal and cognitive mapping methods for the identification of risk in IT development projects. The research was informed by evaluations based on the Delphi data survey, a questionnaire method involving experts in successive rounds to form consensus.

An alternative approach by Fenton and Neil (2005) focused on useful predictive and corrective facets of the risk management process such as for example, predicting the likelihood of a hacker or virus attack. In particular, a major facet that may contribute to the success of effective risk management is to take into account the risk awareness factor within an employee in relation to such facets. IT process risk awareness development needs to be managed via the systematic management of underlying processes. According to Calder (2006) such processes need to be aligned according to the organisation's needs and business objective. This implies a strategic focus in relation to risk awareness in terms of prioritising those facets which promote organisational goals.

A more holistic approach emphasising social dimensions was adopted by Ikram (2000) resulting in an empirical study into the management of risk in IS development, the nature of risks, current risk management practices and their effect on IS development in the UK. Ikram (2000) observed a lack of rigor into risk management research, particularly on the human factor. He defined three parameters that posed the most serious risk issues in information systems; Estimation, Organisation and Personnel Capabilities. However, the model was not tested in a practical implementation as the aim was to develop a theoretical model only. Therefore, Ikram's study did not include an observation of the human factors within the process of risk management.

3.5 Dimensions of Risk Awareness

3.5.1 Situational Awareness

As a major focus of this study is awareness it is important to examine how individuals acquire and manage awareness. A significant emerging concept is Situation Awareness (SA) building on theories incorporating cognitive and human factors. Endsley and Garland (2000) provide a generic definition of SA as perceiving and comprehending the meaning of environmental elements within the boundaries of time and space, in conjunction with the ability to project their status in the near future. A wide range of situation awareness definitions emphasise the integration of knowledge and drawing on information and behaviourial stimuli from their situation contexts (Emerson, et al, 1987; Harwood et al., 1988). According to Taylor (1990) situational awareness is the knowledge, cognition and anticipation of events, factors and variables critical to the success of a mission. Meanwhile, Harwood et al., (1998) synthesised the findings from a range of studies involving the concept of situation in relation to temporal and spatial awareness. In a policing IT context for instance temporal awareness might concern knowledge of cybercrimes developments and events over time and the evolving security implications. The spatial element emphasises a multidimensional understanding of security threats.

In a practical sense this implies awareness of cues in the environment and identifying what might then occur or the consequences of a certain course of action. Situation awareness establishes a basis therefore for risk awareness. This relationship is emphasised by Stanton et al., (2001) in stating that any situation in which human beings need to track events requires effective situation awareness. The growing importance of situation awareness is underlined

by increasingly complex and dynamic systems, information flows and new technologies in many domains in which poor decision-making can have significant consequences. This is evidenced in the high risk field of aviation, where Endersley and Robertson (2001) report that 88% of pilot error is attributable to lack of or errors in situation awareness. Naderpour et al., (2014) emphasise situation awareness as the basis for engaging in effective decision-making activities and point to a lack of situational awareness as a cause of many workplace accidents. Logically therefore situational awareness could be argued as a significant factor within risk awareness as without a wider sensibility of the environment and current or future situations it is unlikely that risks will be apprehended and understood in a comprehensive way.

As such it is argued that a human-centric approach is needed to support situational risk awareness and understanding and assessment of current situations and the appropriate action. Lee (2009) further underlines the importance of a human-centric approach in arguing that emotions can influence situational risk awareness. A small but growing body of literature addresses the theoretical and practical application of situation awareness in diverse domains. However within the field of information systems and IS risk there is a substantial dearth of situational awareness research which means that as yet the importance and dimensions of situational awareness for IS risk awareness and assessment remain to fully defined and understood. Webb et al., (2014) underlines the significance of a situational awareness approach for information system risk managers. It is asserted that common negative tendencies in relation to risk assessment such as perfunctory risk identification and risk estimation with limited reference to organisational situation can be attributed, at least in part, to a lack of situational awareness. This is because these problems identify ways in which information associated with the entity´s IS risk environment is not being perceived or comprehended (Webb et al., 2014). Significantly models of risk awareness are emerging which include or combine elements of both situational and risk awareness. Naderpour et al., (2014) propose a situations risk awareness approach for process systems and operator safety utilising a mathematical model involving fuzzy risk estimation calculations which proposes to address risks from systems failures and reduce human error in risk decision-making. The model is empirically tested and found effective in meeting the requirements of a practical situation awareness system however the utilisation of a single case organisation potentially weakens the overall result.

Webb et al., (2014) proposes a situation awareness model for information security risk management involving the organisation-wide collection, analysis and reporting of risk-related information. Again using a single case organisation to empirically test the model it was found that it held explanatory power and provided a generic template for the incorporation of situational awareness within organisation-wide IT risk awareness strategies. A number of challenges were highlighted including timeliness of information, resourcing, difficulty of analysing and synthesising risk-related information from across the entire organisation, and acquiring the necessary information from stakeholders (Webb et al., 2014). The latter issue highlights that attention to enterprise culture in terms of openness, communication and information-sharing could be important aspects in promoting risk awareness. The Information Systems Audit and Control Association (ISACA) (2009) states that many enterprises develop and implement technology policies, processes and standards with limited understanding of the impact of organisational culture on programme effectiveness.

3.5.2. Cognitive and Psychological Influences

In the information technology domain Rhee et al., (2012) note the damaging trend of increased vulnerability to information security threats coupled with limited managerial action to address the issue. Moreover Siponen (2000) notably highlights that despite risk awareness and knowledge of information security guidelines employees frequently fail to apply them in the manner in which they are intended. This is supported by recent evidence which shows that 70% of employees admitted to frequent disregard of IT policies (Cisco, 2011). These findings emphasise issues within managerial and employee risk awareness which are potentially interfering with the undertaking of appropriate risk actions.

Research has pointed to a number of cognitive, emotional and psychological aspects of risk awareness which can influence risk perceptions and consequent behaviour. Findings from the literature indicate that cognition of risk can be subject to a range of different biases which influence awareness and estimation. Optimism bias is one prominent example which refers to individuals´ tendencies to underestimate the potential for negative events to happen to them, demonstrating a belief in personal invulnerability and lower exposure to risk than others (Weinstein and Klein, 1996). Studies have shown that optimism bias can have important consequences such as exacerbating risk-taking (Adams 1999; Erenberg, 2005) and

undermining preventive actions and precautionary behaviours (Schwarzer 1994; Helweg-Larsen and Shepperd 2001).

Rhee et al., (2012) point to the impact of optimism bias in an information security environment among management information system executives. The findings, drawing on a robust cross-industry sample of 204 executives, show that a modest level of awareness and commitment in relation to information security threats is directly influenced by optimism bias, with executives perceiving their information security risk as significantly lower than comparators. The results indicated that MIS executives understood the reality of potential information security risks but were reluctant to apply that reality to them. Moreover the study highlights that managerial perceptions of the controllability of the risks influenced optimism bias and was itself shown to be exaggerated (Rhee et al, 2012), implying unfounded beliefs not only in greater invulnerability but also in increased capability to manage and control threats. These results are supported in a field survey implemented by America Online (AOL) and the National Cyber Security Alliance using a more generalised sample (AOL/NCSA, 2004). Interviews and technical analyses were conducted with 329 computer users which highlighted that individuals underestimated virus infection and overestimated virus protection measures.

The findings from these two studies reinforce the robustness of the concept of optimism bias and emphasise that risk perceptions and awareness, however inaccurate or irrational, are significant factors to be considered in the management of risk. Moreover this may imply a challenge for effective risk awareness measures in persuading and motivating individuals to change current behaviour and further be reactive to potential threats (Rhee et al., 2012). However both studies were conducted in the single national context of the US therefore limited insight is provided of the cross-national or cultural nature of optimism bias and if and how it operates in other cultures with similar effects. For example, one potential issue is whether optimism bias is strongly present or has a similar impact in cultures which are more risk-averse. Furthermore Rhee et al., (2012) assert the importance of security awareness training to overcome the impact of optimism bias on risk awareness which it is contended should take precedence over any other security training initiatives. Evidence has shown that ongoing security training is essential in many areas of information security (Dutta and Roy, 2003; Mitnick, 2003). As training is an important aspect of governance this underlines the

significant role this aspect plays in providing the environment to support increased risk awareness.

Another dimension identified in the literature in relation to risk awareness is the effect of emotions and psychological factors on risk perceptions. Slovic (2010) shows that liking or enjoyment of a particular activity can result in lower risk perceptions and higher assessment of benefits while the converse also holds true. This has substantial implications for organisations and IT risk management as risk awareness can therefore be biased in terms of an individual´s role, inclinations, and objectives. Harkins (2012) emphasises that activities which support an individual´s objectives will be viewed as constructive and therefore the potential exists for associated risks to be significantly under-estimated. In the information security context for example Harkins (2012) suggests that the attraction many employees feel towards social media could result in significant distortion of risk and benefit perceptions in relation to the disclosure of role and work information which could be exploited by malicious individuals. To counteract this bias potentially strong compliance and governance controls are required to firstly raise awareness of the risks to the organisation of contravening security policies and secondly of the negative consequences to the individual.

Research shows that a number of other psychological factors have important influences over risk awareness and perceptions. Breakwell (2007) argues that awareness can be impacted by normative effects to the extent that individuals have greater propensity for risk-taking behaviour if they perceive their colleagues as doing the same. This strongly emphasises that enterprise culture is critical in impacting on and shaping risk awareness levels signalling that a focus on this aspect is a crucial element in any risk awareness initiatives. Another identified factor is a feeling of control over situations which Schneier (2008) indicates tends to lower risk awareness in the case that control perceptions are high. With the opposite effect to optimism bias, social bias influences individual risk perceptions to the extent that when others are perceived as in danger our awareness of risk is raised (Schneier, 2008). The diverse range of biases and influences over risk perceptions and awareness underlines significant complexity in understanding and shaping risk awareness. Gerber and von Sohms (2005) argue that these factors encompass the social context in which security controls are applied and user perceptions are formed in relation to risk. Furthermore the literature implies that risk awareness measures could be improved if not only technical but social, psychological and cognitive factors are taken into account.

The concept of moral hazard may constitute a substantial influence within risk awareness and risk behaviour. Moral hazard is a situation in which an individual under partial exposure to risk acts differently than they would if they were subject to the entire consequences of the risk (Harkins, 2012). In an information system context this could equate to taking less care of company-provided laptops than one´s own as costs associated with repair and replacement are borne by the company. Notably a survey by Cisco (2011) showed that 61% of employees did not perceive any responsibility for protecting devices or information assets, which were viewed as the remit of IT departments. The identification of this type of perception is important for risk awareness as it suggests that employees are potentially prepared to neglect or ignore risk awareness information or further rarely engage in proactively informing themselves of risk. This further argues for a risk management approach through which can be applied a range of processes and tools including managed and mandated risk awareness programs. Moreover the role of enterprise dimensions in counteracting moral hazard tendencies is potentially significant. Enterprise-wide risk management can ensure that tools and measures are implemented enterprise-wide while a focus on enterprise culture could result in an environment which discourages such attitudes.

3.5.3 Enterprise Risk Awareness

Another dimension of risk awareness is its application in an enterprise context and its resulting efficacy in terms of lowering harmful incidents across the organisation. Risk awareness is argued to be effective in organisations only when practiced across the enterprise by every member (Stoney, 2007; Standard and Poors, 2005). Bayaga and Moyo (2009) emphasise that consequently a culture of risk awareness needs to be created and reinforced at every level of an organisation. This is argued to involve leading by example and the implementation of reward and compensation systems connected to risk awareness practices. Consequently the literature supports a focus on enterprise dimensions, specifically an embedded risk awareness culture, as a central plank of enhancing risk awareness levels. Moreover the need to draw on governance and risk management procedures and processes is implied in the implementation of programmes to support risk awareness.

Studies have further shown that risk awareness across organisations is influenced by organisational actions. For example Bayaga and Moyo (2009) using a mixed methods

approach present evidence which indicates that organisational preparedness in terms of understanding and documentation of risk policies and practices and action plans to treat risk were significant and direct factors in raising enterprise-wide risk awareness. A potential key conclusion is that IT GRC could significantly support risk awareness through systematising and automating many of the processes involved in organisational preparedness. Key results from an industry survey have shown that a lack of coordination and integration of these elements challenges the creation of risk awareness across the enterprise and at board level (KPMG, 2011). Nevertheless these findings are in the single context of a higher education institution with distinct organisational dynamics which may not necessarily translate into other organisational and cultural contexts. Moreover the study remains largely unsupported as limited research has been conducted exploring the factors and relationship between differing variables associated with risk awareness and preparedness (King Report, 2009). This further points to a potential lack of understanding in the IS context of how organisational action and preparedness can influence risk awareness and to what degree.

In addition to lack of understanding in relation to how organisations can promote risk awareness Poepjes and Lane (2013) assert that in the context of information security a significant lack of knowledge exists in relation to an appropriate level and impact of awareness on the effectiveness of enterprise information security controls. Tsohou et al., (2010) defines these as the rules and regulations which when properly apprehended and implemented are able to prevent or diminish the negative effects of attacks on IT systems. This underlines that evaluation and assessment in the context of enhancing risk awareness is critical to understanding and reinforcing the dimensions which support it. Moreover Lindstrom and Hagerfors (2009) argue that awareness and knowledge of these controls can afford organisations a substantial level of defence. Therefore a lack of understanding of how awareness affects the role and capability of information security controls potentially undermines the impact of controls on information security.

Poepjes and Lane (2013) propose a model to address these issues combining best practice embodied in ISO standards with situation awareness theories to form the information security awareness capability model (ISACM). The value of the model lies in the potential to provide a practical and straightforward methodology for identifying gaps in information security risk awareness which potentially could be used across a range of contexts. The model focuses on three core dimensions encompassing firstly Awareness Importance, referring to the degree of

significance awareness has for the effectiveness of a control or process. A second element is Awareness Capability defined as the individual level of capability when confronted with a decision and links to situation awareness in terms of ability to comprehend the situation. The ultimate element is Awareness Risk which is derived from the difference between the necessary level of awareness (Awareness Importance) and that displayed (Awareness Capability) (Poepjes and Lane, 2013). Nevertheless it is important to note that the model is still to be fully developed and empirically tested therefore overall validity and practical utility remain theoretical only.

3.6. Risk Communication

The effect of risk awareness on risk management depends on an effective risk communication strategy. According to ECHA (2010), the purpose of risk communication is to help in trust building, undertake better decisions, address risks efficiently, initiate efficient deployment of risk management policies, reassure and empower the public, prevent critical situations and manage critical situations when they happen. More than a provision of information (ILGRA, 1998), risk communication is a dual process in which all the involved parties can mutually learn from each other (Science Wise ERC, 2009). Embedded in most definitions of risk communication are concepts which emphasise that risk communication between key different groups and audiences involves active interaction and dynamic exchanges (Infanti et al., 2013). However contemporary practice tends to be less dynamic and mainly involves the passing of quantitative risk information from experts to lay people. Risk experts analyse risk using specialist nomenclature usually involving mathematics and statistics, like 'What-if scenarios' and 'Monte Carlo simulation' and discipline-specific concepts like 'transfer of risk', 'risk register', and 'P-I tables' among others. However lay peoples' perceptions of risk are very different from experts' view of risk. This is emphasised by Borodzicz (2005, p32) who states:

"In contrast to experts, lay perceptions of risk are tied, at least ideally, to a particular set of social, cultural and psychological factors. Lay perceptions are frequently characterised as being construed on the basis of irrational and non-objective models of reality which become validated on the basis of folk theories of risk and danger".

This highlights the danger in uni-dimensional and uni-directional practices of risk communication which fail to take account of the cognitions, emotions and behaviour of the

target audience. Individuals find technical risk information from experts, mostly quantitative, difficult to understand and critically difficult to apply to their tasks and responsibilities. Nevertheless risk communication theorists argue that the divergence between experts and lay peoples' perception of risk exists because of methodological issues. Risk management research is carried out using the scientific research method which requires empiricism and attention to data collection and analysis methods. An alternative risk communication research uses a sociological approach to the study of risk that diverges from quantitative language mostly used to communicate risk. Risk communication theory focuses on the dialogue between risk experts and lay people who are involved in the risk as protectors or in mitigation efforts (Irwin 1995). This sociological perspective is useful for understanding and developing techniques to improve the levels of IT systems risk awareness.

Wynne (1989) argues that deeper social assumptions within which risk communication occurs need to be considered**.** How the message is evaluated depends on the way in which individuals and groups receive it, interpret and analyse the imminent risks (Infanti et al., 2013). Experts make such assumptions in the construction of 'technical risk analysis'; such as 'statistical probability', 'models' and 'random processes'. Such analysis is underpinned by social models which fail to be communicated to lay people by experts and they determine what is regarded as risk and what is not. He asserts:

> *"The point of general importance shown by this case (agent orange pesticide) is that different parties – the scientists and the worker – defined different actual risk systems, or risk analytic problems, because they build upon different models of the social practices creating or controlling the risks." (Wynne, 1989, p.37)*

Critically, experts' assumed social models contain crucial assumptions that may not be verified in practice. They may erroneously assume understanding of the technical information on the part of lay people, acceptance of the identified risks and risk strategies and compliance with risk mitigation strategies.

Responses therefore need to be shaped by understanding and consideration of the individual level factors which may impinge on risk communication. For example risk communication efforts can be challenged by perceptions of risk as according to McInnis (2005) the fact of 'agency' is essential in shaping risk perceptions. The risk perception refers to the feeling

whether a certain action can or cannot be taken to control risk exposure. These factors are responsible for altering the cognitive, emotional and behavioral responses to accept and process risk information, leading the involved parties to display various levels of anger, worry, concern, fear, hostility, outrage and anxiety.

Covello et al., (2001) highlight further individual factors as according to their findings people can tend to enter a high level of stressed state after receiving significant threatening information which impairs their ability to perceive and process the information logically. However Covello *et al* (2001) argue that if the person has an existing 'mental model' to aid them in understanding the risk, the new information is likely to be processed logically and accepted. Therefore the importance of crafting effective risk awareness within risk communication strategies is critically underlined in order to embed a mental model which can be referred to by users in risky situations. It is further argued that understanding of how an audience in highly stressful situations may act is necessary for helping risk communicators translate scientific and technical concepts into messages that are comprehended easily (Covello et al., 2001).

Trust is an underlying dimension identified extensively in the literature as also significant for the effective communication of risk messages. Schuler (2004) argues that trust plays a prominent role in shaping risk perception due to its role in influencing attitudes and behaviours. Therefore risk communication messages and strategies become successful in achieving an end only when they have the trust of the public. On the other hand, trust determination theories espouse that when audiences are upset with the source of information, they do not trust or believe in the authority (Infanti et al., 2013). In order to ensure that future risk events are firmly and effectively handled, a trusting relationship with audiences must therefore be established as empirical evidence shows. A random survey of the Dutch population performed by Huurne and Gutteling (2009) revealed that both institutional trust and the person's trust in themselves influences individual actions. In particular perceived self-efficacy and people's institutional trust influences risk communication. The survey shows that the purpose of risk communication should not only be about building trust in institutions but also to motivate people to believe in self for theefficient handling of risks. In addition, Kahlor (2007) argues that risk information should be relevant to the person as it will contribute to the extent in which the person adopts risk prevention behaviour and establishes long-term change in the behaviour of the person.

3.7 Methods for increasing IT systems risk awareness

It has already been noted that existing research on risk management alludes to risk awareness however few studies utilise risk awareness as the unit of analysis. An even more significant gap in knowledge concerns techniques and methods for increasing IT systems risk awareness among all concerned.

The proposed IT risk awareness conceptual model is a springboard for thinking about methods for increasing IT systems risk awareness. Methods for increasing IT risk awareness based on theory would be more effective, such as the proposed model in this research. However, most available methods are either the creations of pragmatic practitioners or researchers interested in prescribing, and whose research does not include theory. Rather, prescriptions by researchers are generally based on conceptual models.

The available research on increasing levels of risk awareness is predominantly based on methods involving motivation, selling, and prescribing. Motivation and attitude are critical for increasing levels of IT systems risk awareness. "It is traditionally seen that motivation tends to be dynamic in nature (lasting from minutes to weeks) whereas attitude is a more static, internalised factor (lasting from months to years)" (Siponen, 2000: 33). Mclean (1992) suggested "selling" information security to employees through workplace campaigns. These campaigns can be used for security education and potentially have a positive impact on the workforce. However, some security campaigns can result in adverse attitudes including negative feelings, irritation and various forms of resistance to the message given and therefore it is acknowledged that care should be taken (Siponen, 2000).

Siponen (2000) offers 'prescriptive awareness' as a method for increasing IT systems risk awareness. He defines prescriptive awareness as: "a situation where people see (internalise) a norm or guideline as a matter which they are bound and obliged to follow. This kind of accomplishment-oriented commitment can be external or internal as a form of motivation" (p.36) He suggests the following prescription awareness tools would help reinforce the message: logic, morals and ethics, rationality, emotions, sanctions/pressure, feeling of security and well-being. Significantly, motivation, selling and prescription provide people orientated methods for increasing risk awareness.

3.8 Conceptual Framework

A conceptual understanding or model of IT systems risk awareness, the MERIT IT Risk Awareness model is developed. This conceptual model draws on the literature earlier reviewed to extract empirical categories of significance for developing knowledge of IT systems risk awareness. These empirical categories are then used to develop a conceptual model of IT systems risk awareness for effective implementation within organisations.

The five elements of the MERIT conceptual model are significant areas of IT risk management to demonstrate. The model defines governance foresight, compliance behaviour, enterprise coverage, IT systems focus and overall IT risk management. All of these factors are necessary to secure IT systems from threat through enhanced risk awareness. The conceptual model should reflect the nature of IT systems risk awareness in two respects, variability and uncertainty. The variability of a situation is how the events occurring in the situation of interest differ unpredictably. Uncertainty of a situation can involve a lack of knowledge in that area which is also known as epistemic uncertainty. The aim of drawing on conceptual evidence and empirical findings in this literature is to undertake conceptual analysis of IT systems risk awareness. Knippenberg (2011) argues that conceptual analysis has the potential to contribute to theorisation. He supports 'high-quality conceptual analyses based on conceptual evidence and empirical findings to further knowledge. Christensen and Carlile (2009) state that 'theory' is a body of understanding and that the "building of theory occurs in two major stages: a descriptive stage and a prescriptive stage." The descriptive stage consists of observation, classification and defining relationships. Conceptual analysis contributes to the descriptive stage.

The veracity of the proposed MERIT IT Systems Risk Awareness Conceptual Model is underpinned by theoretical understanding of risk management literature. The conceptual model focuses primarily on enterprise IT systems risk awareness. Public and private organisations now have large-scale dependencies on the collection and utilisation of sensitive and valuable data, which they need to safeguard from data security breaches. IT related risks pose significant challenges to enterprises of all sizes, irrespective of the nature of the business private or public, profit or non-profit, large or small. Governance, compliance, enterprise, IT GRC, risk management and risk awareness factors have an effect on individuals' risk

awareness and impact risk management and are significant to understanding IT systems risk awareness.

Figure 2 Elements of Risk Process

This research proposed five dimensions to reflect the management of Risk Awareness. Tarantino (2008) lists three elements as Governance, Compliance, and Risk Management in no specific order. Pohlman (2008) lists five elements as Governance, Compliance, and Risk Management, Enterprise and IT GRC in no specific order. The elements of these processes including the Risk Awareness element are depicted in Figure 2. These elements or interrelated processes result in the risk awareness outcome. The argument and logic underpinning the illustration in Figure 3 is based on employees' risk awareness. Previous studies have identified these elements however they have not focused on the people aspect of risk management and in particular staff risk awareness. This provides a potential new perspective to this research. The order of the elements in the Figure 3 pyramid is significant, because the unit of analysis is people or staff. Staff should be aware of the governance policies of the organisation which is the bottom level; this includes the awareness of governors of IT systems risk. They are then required to comply with the policies, which is the second level of compliance to the requirements of risk management. Staff should be familiar with organisation or enterprise business processes, which is the third level. For IT staff, these three levels; governance, compliance and enterprise, form the IT GRC fourth level of the

pyramid. This then enables them to understand IT systems risk management which is the fifth element. When all levels of staff understand and comply with all these five elements, then they can be said to be risk aware, the final top level of the pyramid.

The conceptual framework can also be stated in a more integrated holistic manner. Under Figure 4 the enterprise dimension reflects the strategic alignment and organisational wide dimension which embraces three strands of governance, compliance and risk management. IT GRC reflects a specific integratation and standardisation of structures and processes. The design and implementation of these dimensions are modelled as impacting on risk awareness and influencing the level of awareness. Monitoring processes within and the culture of these dimensions can increase the visibility of information system assets and awareness of threats. At the same time risk awareness can inform the design and implementation of these components through an iterative process. The dynamic nature of risk awareness incorporating cognitive, psychological, behaviourial and socio-cultural elements is depicted in Figure 4.

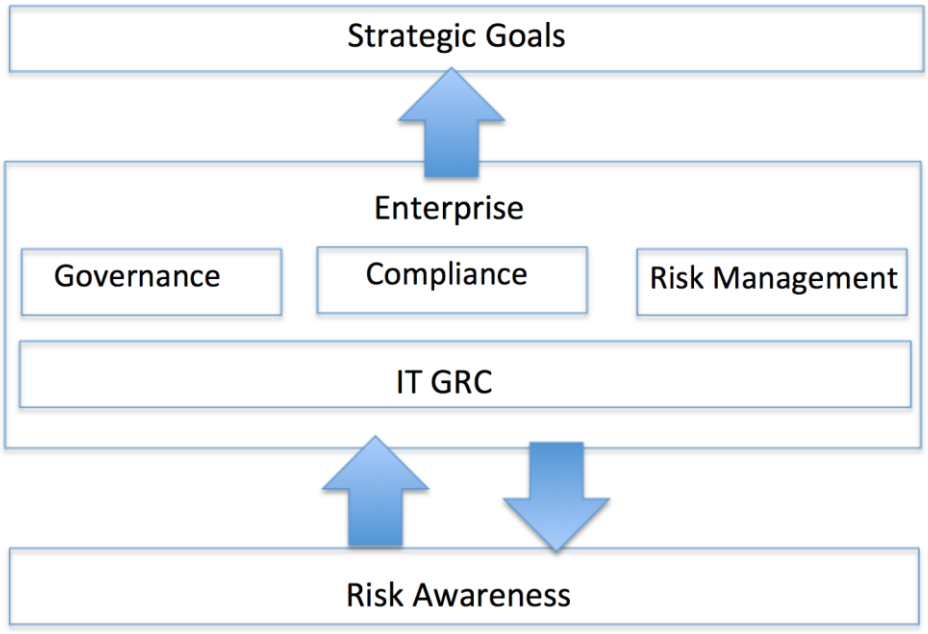

Figure 3 Structural Model (Author's Own)

This conceptual model provides new knowledge and shows the risk processes related to five elements that are currently in practice in private and public organisations. Governance, compliance, enterprise, IT GRC and risk management should result in the enhancement of managers' and staffs' risk awareness. These elements are defined and elaborated below. They

are types of risks related directly to IT systems risk awareness, which, if not managed, could well occur.

Figure 4 Conceptual Model

3.8.1 Governance

Governance is a significant dimension for this model as it is noted as a key tool for connecting the structures and processes of an enterprise (Cavalcanti, 2014). Governance is the system by which organisations are directed and controlled. Governance mechanisms are defined as structures or processes which enable responsible functions for making appropriate decisions. Governance for IT projects or departments means the risk reduction and increase in business value generation through utilisation of information technology infrastructure in the organisation (Bowen et al, 2007).

An awareness of risk as the basis to identify and manage risks has become an increasingly critical dimension of governance for modern organisations. Thanopoulos (2014) notes the continually evolving framework of knowledge underpinning decision-making. Consequently the state of flux which characterises the business environment emphasises the importance of risk awareness as a conduit which feeds into the governance systems to guide and direct change. As Thanopoulos (2014) notes quality data is vital for drawing conclusions. The governance dimension in the MERIT reflects the strong relationship between the situation and risk awareness and the capacity of employees to effectively identify and assess risks. Emphasis of enterprise-wide consultations with employees to develop higher levels of risk awareness has been noted (Coyle, 2004). Governance is essential to improving the overall effectiveness of boards and managers and is critical to embedding a risk culture which can impact the level and effectiveness of risk awareness and in turn impact on effective management of risk. Evidence shows that the presence of strong governance can significantly enhance risk awareness and communication supporting an enterprise-wide culture of risk-awareness. Moreover improved quality in risk information and better coordination of functions essential to the promotion of risk awareness such as risk and compliance are noted (EIU, 2013).

3.8.2 Compliance

Information management and security is key issue given the pervasiveness of IT in all aspects of society where data is stored and accessed an interconnected and interdependent network of systems. Compliance is concerned with standards, policies and procedures for the internal management and responses to external forces in an organisation. The significance of compliance can be illustrated by its proportion of IT budgets which has been as high as 40% for organisations such Barclays Bank (Riley, 2004). According to Masing (2009, p.48):

> *Major compliance regulations recognise this (core business processes) and require executives to implement risk assessment and internal control systems for their enterprise's information technology. IT risk management practice often needs to reduce the number of blind spots to risk, keep up with changes in the IT landscape and reduce risk assessment costs.*

Both internal and external compliance represent major sources of information management and security risks. A key driver which heightens risk for organisations is continually evolving nature of technology and external legal requirements. The complexity is compounded when operating across different geographic boundaries and regulatory and legal contexts. Risk awareness forms a vital component in maximising adherence to internal and external compliance standards and regulations.

IT security perspective provides a compelling basis for the integration of compliance into the MERIT risk model for this study. Organisations face significant security threats which manifest from adversaries both external and internal to the organisation to exploit and cause damage to assets (Agrawal et al., 2014). The daily dependency on IT systems can be threatened by a myriad range of risks. Moreover, a single threat can result in multiple negative impacts (Agrawal et al., 2014). Compliance within an organisation mandates that employees need to observe the requirements of government systems and adhere to the policies in order to reduce any risk. Internally there is a requirement for a good level of knowledge concerning the consequences for failure to adhere to operational policies and procedures (Andress, 2014). In the context of policing lack of awareness of both potential threats and risk to forensic or case management and new developments can have significant repercussions for justice and public safety. From a regulatory perspective compliance implies up-to-date knowledge of relevant IT regulatory requirements and developments.

Risk management methodologies like the maturity model framework for enterprise risk management (ERM) proposed by Abrams et al., (2007), have compliance risk management as a significant component. Similarly, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework has compliance as a major component of risk management. COSO framework application provides enterprise risk and governance control for a wide range of issues such as internal controls, appropriate financial reporting, performance targets, to prevent loss of resources, ensure effective reporting, and compliance with laws and regulations.

3.8.3 Enterprise

The enterprise dimension forms a significant component of this model in order to account for the interdependent and interconnected nature of organisations. This recognises risk awareness

as an enterprise-wide consideration. Rapid developments and technology create pressures for organisational change and emphasise the importance of risk management (Hampton, 2014). An enterprise perspective reflects an organisation-wide holistic view of risk awareness. Enterprise risk management leverages three main organisational aspects of people, processes and technologies to design, deploy and sustain a unified risk infrastructure. An enterprise view of risk awareness recognises the significance of alignment of the business model, and the spanning of risks across multiple levels and organisations units and roles.

A key premise is that risk awareness is not centrally managed or localised to single risk managers but should permeate across the enterprise. This is supported by Hampton (2014) who argues that risks should not be addressed single owners (Hampton, 2014, p145). Enterprise risk awareness maximises both the identification of threats and opportunities. The term 'enterprise risk management' (ERM) captures this purpose well. ERM entails developing proper risk behaviour in all employees, including managers and the risk managers themselves. Finally, this dimension addresses the issue of departmental and functional risk silos and the significant misalignment between business and risk functions evidenced many organisations (EIU, 2013).

3.8.4 IT GRC

IT GRC refers to a unified, comprehensive and inter-connected approach towards **G**overnance, **R**isk Management and **C**ompliance concerning the organisation's use of IT. The governance, risk and compliance in IT GRC refer specifically to the adoption and use of IT by the enterprise. The integration of IT GRC into the MERIT model recognises the significance of information security, IT compliance, data and risk management in aligned manner highly relevant to policing operations. IT GRC compels businesses to make use of IT to present a unified, comprehensive, and inter-connected approach towards a successful enterprise. The major factor within this element is using the skill and effectiveness of IT to its maximum advantage and latest developments. Risk awareness facilitates the integration of a wider culture of security and risk awareness enterprise-wide which is aligned to the external dynamic context which the police forces face. This dimension is significant as a new awareness of risk is emphasised which can be informed by a strategic and operational framework facilitated by IT GRC in integrating current technologies allowing IT GRC processes to be automated.

3.8.5 Risk Management

The incorporation of risk management into the MERIT model establishes a frame of reference for key risk management processes informed risk awareness. Risk awareness impacts key processes of risk management in the achievement of organisational objectives in relation to: identification, quantification and management of risk (Hickson and Owen, 2015). Planning, identification and analysis of risk are key stages in this process culminating in the development of responses strategies monitoring and control (Kerzner, 2009). At the identification stage knowledge and awareness of the situation and context can maximise the effectiveness of this activity. Further, the selection of appropriate responses is impacted significantly by the level of risk awareness. This aspect of risk management is critical to developing risk awareness as communication and learning are fundamental aspects which promote greater comprehension and awareness of risks. For example identifying and assessing risk in the external environment is reliant on the maintenance of an effective network of communication with contacts and information sources to enhance identification of changes which could potentially impact the enterprise´s risk profile.

Evidence shows that applied effectively risk management can support the organisation to identify and comprehend uncertainties within business strategy and in the competitive environment partly as a result of horizon scanning activities (Power et al., 2013; Mikes et al., 2013) which is contingent of awareness of risk.

Qualitative studies of risk management include Al-Fehaid (2003) who empirically investigated the impact of IT-based accounting systems on the audit function and the potential risks for auditing. With no available theoretical base to use, Al-Fehaid used the grounded theory inductive approach to develop and test a theoretical model. Notably Al-Fehaid's findings concur with the governance and training variables of the MERIT IT risk awareness model of risk management proposed in this research. Moreover the findings supported the variables that influence the level of audit risk in IT-based accounting and the relationships among the variables, and concluded that the adoption of IT-based accounting systems by firms has 'contributed to possible increase in audit risk.' Al-Fehaid explains that the risks may be due to the accounting software, untrained staff or inadequate internal control systems

3.8.6 Risk Awareness

Risk awareness is the 6th component of this model representing a cross-cutting and comprehensive dimension underpinning other dimensions. Understanding of risk awareness and the impact of model dimensions is understood to require some form of measurement in order to identify priorities, discrepancies, and conditions which promote risk awareness. It has been noted that monitoring and evaluation is essential to refining approaches and methods and understanding the effectiveness or shortcomings of different factors on risk awareness (IFRC, 2011).

The central premise is that risk awareness levels in each of these areas critically impact on the effectiveness of functions and the overall organisational success. These five dimensions (governance, compliance, enterprise, IT GRC, risk Management) represent five major areas of IT management which have become increasingly dependent on new awareness of risk. These dimensions present a holistic frame of reference for exploring risk awareness. While there is a significant overlap between the general governance, risk management compliance dimensions and specific governance within IT GRC, both have relevance. While IT GRC focuses on IT specific related governance risk, an understanding of risk awareness issues within broader compliance, governance and risk contributes to holistic strategic exploration of risk awareness. Risk awareness within the MERIT model represents the central connecting underpinning dimension impacting on the effectiveness of the five other dimensions. Since awareness is a human quality, this element focuses on measuring the effect of the previous elements on managers and staff level of awareness of risk.

Table 2 Merit Model Factors

Factor in the MERIT model	**Finding**	**Previous researchers supporting this study**
Risk awareness	The risk awareness is an overarching outcome of any risk mitigation mechanism or training implemented across departments in the organisations. It depends on the following sub functions such as governance and compliance.	Pember, 1996; Bowen et al, 2007; Vose, 2008; Rush and Vednere, 2008; Bakker et al, 2011
Risk management	The success of risk management largely	Ikram ,2000; Kutsch, 2005;

	depends on assessment, identification and compliance along with training and performance of employees. It directly affects the risk awareness status of the organisation.	Allan, 2007; Dey et al, 2007; Taylor, 2007; Gottschalk, 2010
Governance	Governance depends upon feedback, implementation time take and guidance provided to and learning outcome of employees. Skills, experience and performance of the employees increase the quality of governance implementation and its utility.	Bowen et al, 2007; Christopher, 2010
Compliance	Compliance depends upon application, training and guidance given to employees and feedback received post-implementation of governance mechanisms and compliance and standards.	Riley, 2004; Abrams et al, 2007 Masing, 2009
Enterprise	Enterprise comprises risk management as a component. However, main aims of business organisation such as quality, customer satisfaction and size of the organisation affect the enterprise value and in turn impacts how risk is managed.	Hilson, 2006; Rau and Haerem, 2010; Young, 2010;
IT GRC	IT GRC is about managing IT risk and separately implementing governance and compliance in IT projects and usage so as not to affect the risk awareness negatively for the overall enterprise.	Schmidt et al, 2001; Kumar, 2002; Stoneburner et al, 2010
Risk management process – identification, assessment and	The process of identification, assessment and control depends upon the training, performance of employees and systems and time taken to respond to external and	Tesch et al, 2003; Huang et al, 2004; Borodzicz, 2005; Graham and Kaye, 2006

control	internal changes by the enterprise.	

3.9 Conclusion

Many of the studies reviewed above mention 'awareness' as an issue in risk management explicitly or implicitly (Rush and Vednere, 2008; Al-Feaid, 2003; Stoneburner et el., 2002; Siponen, 2000; Ikram, 2000; Straub and Welke, 1998; Pember, 1996; Straub and Welke, 1992; goodue and Straub, 1991; Dixon et al., 1992; Earl 1996). The unit of analysis of these studies were 'enterprise' or 'risk', none of the studies had risk awareness as the focal unit of analysis. The present research takes risk awareness as the unit of analysis and applies it to IT systems and unlike the studies discussed above, also uses a quantitative as well as qualitative approach. The literature review reveals a limited number of studies carried out here shows that there are only three projects relevant directly to the present study (MERIT). These three projects described below span between 2000 and 2008. For the past 3 years there has been no relevant project identified on risk awareness in line with MERIT.

A number of concepts relating to risk awareness have been shown to have significant implications and influence over risk awareness. Risk awareness itself has not been researched extensively and this is a gap in the research literature. Only Gibson (2003) mentions Risk Awareness explicitly out of the literature reviewed. One of the more critical aspects of basic management skills is risk awareness. Risk awareness is a combination of vulnerability assessment and knowledge management which provides critical input to the risk identification and risk management process (Gibson, 2003). Therefore, each organization should have their own risk awareness programme to avoid any uncertain events and develop appropriate risk attitudes. It requires an understanding of the purpose and value of risk management within the business, in order to implement effective risk management within their area of responsibility, and to support its use by others.

Chapter 4 Research Methodology

4.1 Introduction

This chapter details the research methodology adopted to address the research goal towards the development and validation of the MERIT IT systems risk awareness model. The rationale underpinning the research approach and influence of epistemological assumptions is discussed followed by an explanation and justification of the mixed method case study based research strategy and methods adopted. The latter half of this chapter outlines the data collection procedure, sampling, ethical considerations and overall validity and reliability of the study.

4.2 Research Approach

One of the major discussions within philosophy centres on the debate surrounding epistemological and ontological issues (Blunden, 2009). Scientific research is strongly based on epistemological assumptions which assert evidence of knowing and moreover a coherent structure of epistemological, ontological, axiological and methodological reasoning which can direct research (Cresswell, 1998). Research philosophies reflect underlying assumptions in relation to the nature of reality and validity in knowledge which in turn influence the research design from initial phases to conclusion (Easterby-Smith et al., 2012). Consequently reflection on differing philosophies is important to understanding and ensuring the adoption of an approach congruent with achieving the research goals (Blaikie, 2000). Saunders et al., (2009) argue for a practical approach to the selection of a research philosophy in asserting that the highest priority should be the research question. Blaikie (2000) further underlines the significance of aligning research approach and design with the research problem to avoid incoherence within the study.

Three main philosophical perspectives have been considered reflecting differing ontological and epistemological views influencing the underlying approach to this research. Blaikie (1993) suggests that in social sciences research ontology involves claims on what exists, its nature and characteristics, what units it is constituted of and how these interact. Ontological perspectives are generally divided between two different positions asserting either that reality is concrete and external and exists independently of human perception, or that reality is subjective and exists only in human consciousness (Saunders et al., 2009). Selection of an

appropriate research approach further involves epistemological assumptions on the most appropriate ways of inquiring into the nature of reality (Easterby-Smith et al., 2012) and is informed by and depends on the ontological position adopted (Hatch and Cunliffe, 2006). According to Eriksson and Kovalainen (2008) epistemology involves questions regarding what constitutes valid knowledge and its sources and limits and further assert that perspectives on these issues impinge on the research methods selected. A fundamental epistemological issue is whether the social world can be studied utilising the same principles, methods and philosophical approach as the natural sciences (Bryman and Bell, 2007).

One of the principle research philosophies, positivism, links to the ontological belief in the concrete and external nature of reality which accordingly can be measured in an objective manner unrelated to context (Bryman and Bell, 2007). This provides the basis for the formulation of laws and generalisable conclusions (Remenyi et al., 1998) which in turn offers an appropriate scientific foundation for the generation of a broadly applicable model of IT systems risk awareness. Positivist research can further support the investigation of causal factors in IT risk management practices and their observable outcomes such as risk awareness in a quantifiable manner which can be numerically analysed (Remenyi et al., 1998). Positivistic research has the advantage of being able to provide wide coverage of a range of situations, nevertheless positivistic methods can be inflexible and artificial and may fail to provide a deeper understanding of the processes related to IT risk awareness and management or the significance and meaning which the actors involved in risk management attach to actions (Saunders et al., 2009). This suggests that positivistic approaches may not be fully suited to exploring the deeper significance and influence of the factors involved in the understanding, usage and level of risk awareness and impact on the quality and success of risk management.

The contrasting position of interpretivism emphasises humans as social actors (Bryman and Bell, 2007) and contends that reality is socially constructed, multiple, and only properly understood in the context from which it emerges (Wimmer, 2012). Therefore it is perceived as important for the researcher to understand the interpretation and meaning which actors attach to social phenomena and the contextual factors which determine and influence these meanings, which is viewed as possible mainly through qualitative research methods (Saunders et al., 2009). Such an approach can potentially provide a more in-depth, insightful and richer understanding of the specific social situation of IT system risk awareness within

the sample police force (Easterby-Smith et al., 2012). However the significant focus on context and socially constructed meaning potentially limits wider generalisability of the research findings (Saunders et al., 2009).

Therefore consideration of both positivism and interpretivism suggests potential methodological constraints for the achievement of the research objectives. Another perspective is realism which incorporates elements of both philosophies in accepting the positivist argument that phenomena and events exist independent of human thought and experience, while asserting that knowledge of them is created through social conditioning (Saunders et al., 2009). Hatch and Cunliffe (2006) argue that realism focuses on explaining phenomena in the social world through understanding the social structures from which they have emerged and how these may empower or constrain social actors, in addition to how these can be critiqued and changed. Realism further posits examination and understanding at multiple levels and different angles in order to contribute to knowledge (Chia, 2002). Nevertheless realists assert the importance of a scientific approach to the development of knowledge which implies that social phenomena can be studied empirically using quantitative methods. In contrast to positivism, however, realism focuses more on explanation and understanding than prediction (Blaikie, 1993). This provides the basis for a research approach combining the flexibility of interpretivist theories to examine social phenomena while grounded in the empirical approach which characterises positivism.

On balance, consideration of the three research perspectives has led to the adoption of a realist view as the most suitable for answering the research questions. A significant advantage of adopting a realist perspective is the endorsement of a mixed methods approach to research which can be selected in accordance with the type and goals of the project (Zachariadis et al., 2010). Given the multi-layered and multi-dimensional nature of this research the value of utilising mixed methods lies in the ability of the different methods to mutually inform each other to reveal relationships between context-specific practices and changes that are happening at another level of analysis (Kaplan and Duchon, 1988). This means that the research questions can be linked in multi-level analysis and the findings may be systematically cross-referenced. Zachariadis et al., (2010) claim that mixed methods research provides strong cases for basing proposals for change at practice or policy levels.

4.3 Research Strategy

A mixed method case study based strategy combining quantitative and qualitative methods has been adopted. A case study has been defined by Yin (1994) as: "an empirical enquiry that investigates contemporary phenomena within its real life context especially when the boundaries between phenomenon and context are not clearly evident."(p.13). The case study method utilising a range of research techniques has been used to study risk management. This approach facilitates the collection of data on a research situation from a small number of organisations using multiple data sources. The case study approach helps to generate empirical and in-depth qualitative data depending on the methods employed (Yin, 1994) and is widely employed in management research studies (Gummesson, 2000). Case studies are *"of particular value in situations with a relatively underdeveloped theoretic base or where complex observational tasks are involved and it is necessary to capture the complexity or dynamism of the context or organisational setting"* (Harrison and Leitch, 2000). This is particularly justified given the subjectivity surrounding risk awareness identified in the literature. In research cases where an in-depth analysis is necessary, the case study approach is highly recommended as they answer the questions of 'how' and 'why' or when it is difficult to differentiate the organisational context from the research phenomena (Yin, 1993). Given complexity of the organisational context in relation to the research topic a case study strategy offers the opportunity to gain a holistic view of risk awareness multiple methods focused on specific objectives (Eisenhardt, 1991; Gummesson, 2000; Yin, 1994).

This strategy is significantly informed by Creswell and PlanoClark (2007) who explain that mixed methods research can be viewed as both a methodological approach and a method in itself. From a methodological perspective mixed methods research is underpinned by philosophical assumptions which influence the means and methods used to collect and analyse data and the combination of qualitative and quantitative approaches. When considered as a method the principal assumption is that utilising a blend of both quantitative and qualitative approaches contributes more enhanced understanding of research problems than can be obtained from a single approach alone (Creswell and PlanoClark, 2007).

A mixed methods research is associated with a number of advantages over traditional research structures. Principally the opportunity to compensate for weaknesses in any one specific approach is afforded (Jick, 1979). For example quantitative research is more

removed from participants and is limited in terms of providing understanding of contextual factors. These limitations can often be mitigated in the increased interaction with research participants characteristic of qualitative research which enables a more in-depth understanding (Creswell and Plano-Clark, 2007). In contrast qualitative research can engender greater risk of bias in the degree of subjective interpretation required which is balanced by a broader use of participants in quantitative research. Therefore in supporting the combination of a range of methods, philosophical assumptions and theories mixed methods research is able to provide a more holistic and complete understanding (Creswell and Plano-Clark, 2007).

In particular, the choice of method is influenced by the data required to best address the research objectives which in this study utilises both quantitative and qualitative methods. Quantitative research methods have been used extensively in risk management research to facilitate standardised and measurable data which lend themselves to empirical conclusions (Saunders et al., 2009). The emphasis on scientifically-derived objective data offers the potential to make inferences on the collective understanding and practice of risk management within the UAE based on the sample population (Easterby-Smith et al., 2012). Quantitative research is concerned for example with the percentage of employees or managers who indicate a high level of risk awareness. Despite the acknowledged authoritativeness and legitimacy of quantitative methods it can therefore run the risk of overlooking critical knowledge and understanding. Quantitative methods are limited in providing sufficient insight through numerical representation of the complexities involved given the psychological, behavioural, social and cultural dimensions identified in the literature in relation to risk awareness.

This factor underpins the rationale for adopting a qualitative approach. In contrast qualitative research aims to capture the subjective understandings of reality from the perspective of the participants (Easterby-Smith et al., 2012). This allows for gaining greater comprehension of the perceptions of participants in relation to IT system risk awareness and its influence on risk management effectiveness. Qualitative data is non-standardised data based on words and meaning and are often richer and able to offer a more rounded view of a social phenomenon (Saunders et al., 2009). Easterby-Smith et al., (2012) explain that qualitative research enables a more informed and detailed view of perceptions, attitudes, feelings and motivations for behaviour which is highly relevant for this research in terms of gaining deeper insight into

risk awareness and resulting conduct. A qualitative approach focuses on individual cases and the human perspective and understanding embedded within those cases and questions the why and how of factors in relation to risk awareness. This approach allows for the intricacies of the social aspects of organisational contexts in relation to risk awareness to be clarified and understood by means of a more in-depth and comprehensive investigation.

4.4 Research Methods

In line with the methodological design outlined in the previous section the research draws on several methods in order to address the research objectives of this study. Figure 5 outlines the research methods, data collection and analysis underpinning the research outcomes of this study. The research design incorporates three key methods: structured questionnaire survey, in-depth interviews and Delphi panel method. Quantitative and qualitative methods are applied to collect data to obtain multiple evidences in this study. The application of triangulation in terms of methodology and data enables data analysis from multi-methods. Data has been collected through survey within the focal organisation Abu Dhabi Police (AD police), individual interviews and questionnaire survey of 10 UAE enterprises (UAE) and Delphi consensus survey for variables of governance – compliance – enterprise – IT GRC and risk management between experts.

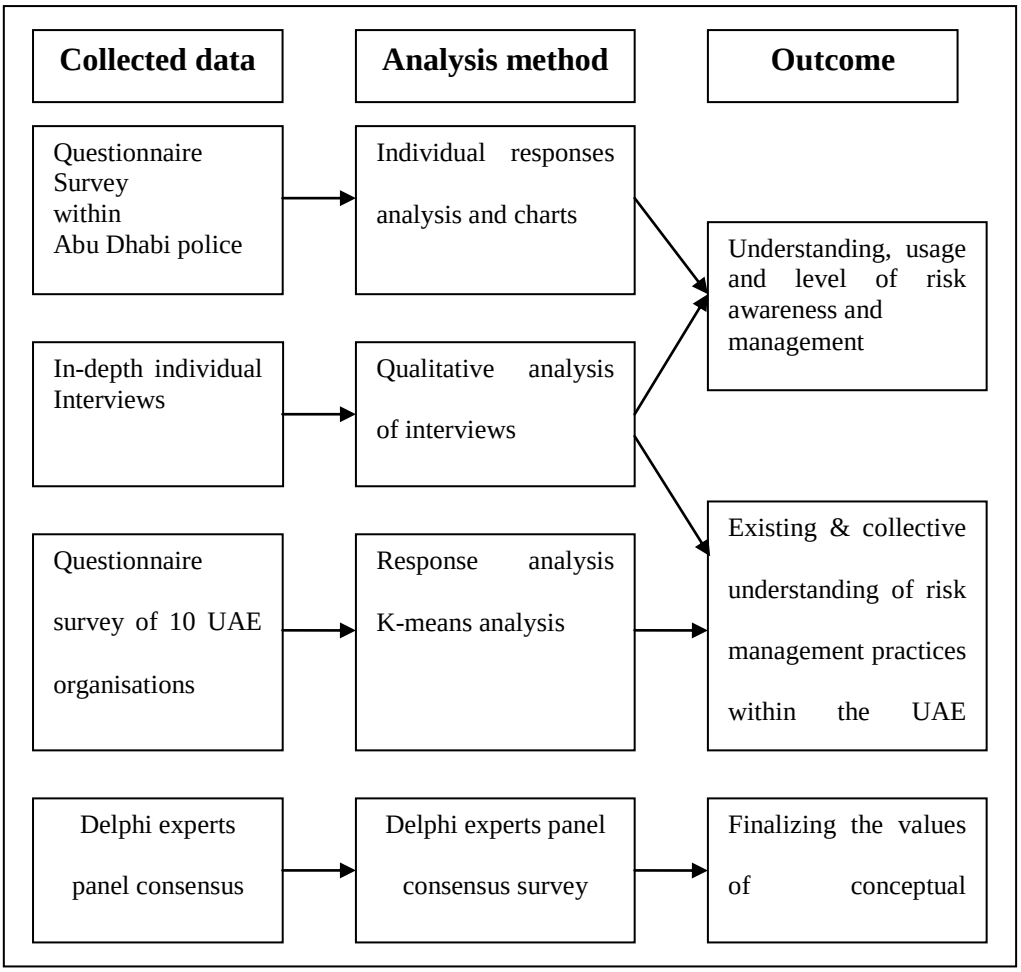

Figure 5 Data analyses strategy (Based on Saunders et al, 2009)

4.4.1 Structured Survey Questionnaire

A structured survey questionnaire has been adopted for the data collection across a number of organisational cases. This method has been widely employed in business and management studies and facilitates the collection of large and comparable datasets in an objective manner (Saunders et al., 2009). The survey instrument is orientated towards evaluating the risk management approach, attitudes and level of risk management knowledge within a UAE police force. This structured approach offers the opportunity to pre-arrange a list of topics providing a clear topic focus in relation to risk management and awareness (Saunders et al., 2009). The adoption of a standardised format of questions and structure response increases the potential for questions to be interpreted consistently and to provide relevant and meaningful responses as well as offering efficient data collection.

Two structured survey instruments were developed. The first instrument targets the ADP and questions sought to probe the participants' understanding of the importance of defining risk

for the purposes of planning and to prevent escalation to problem or disaster status. Responses provided the basis for greater in-depth analysis in later stages. The questionnaire was also used to investigate the attitude of staff in the Abu Dhabi Police Force IT Department sourced from concepts established in the risk management literature. Questions were devised to examine knowledge and deepen understanding of risk, and perceptions in relation to identification and control. A particular emphasis related to attitudes in relation to risk awareness. The questionnaire and the data are produced in Appendices B in English and C in Arabic.

A further structured questionnaire was designed to collect data on risk management from ten small, medium and large private and public sector organisations currently implementing risk management in the United Arab Emirates (Appendix B). Professionals from both private and public sector organisations formed the sample population drawn from small (Case8 to Case10), medium (Case5 to Case7) and large (Case1 to Case4) companies in Abu Dhabi. The questions were focused on compliance and formulated in accordance with research guidelines underlining clear, brief and unambiguous questions to avoid misunderstanding or misinterpretation (Saunders et al., 2009). The questionnaire utilised a 5 point Likert-type scale to measure responses enabling respondents to indicate the extent to which they agreed or disagreed with the risk management statements. The questionnaire contained 119 questions structured according to the following six elements: Governance, Compliance, Enterprise, IT GRC (Governance, Risk Management and Compliance), Risk Management and Risk Awareness. Each element had a set of questions that targeted Risk Awareness, the unit of analysis. The risk management scale was validated by opening it to expert scrutiny. The survey was undertaken among UAE enterprises who currently implement risk management.

Each of these elements was broken down into subsections according to structure in Table 3.

Table 3 Elements and Number of Questions in Survey

Element 1: Governance	**Number of Questions**
A. What is Governance?	4
B. How many types of governance models?	2
C. How does Risk Management relate to Governance?	5
D. The impact of Risk Awareness on Governance	3
E. The impact of Governance together with Risk Awareness on the organisation success	1
Element 2: ENTERPRISE	
A. What is Enterprise Risk Management (ERM)?	4
B. Why implement ERM?	2
C. ERM and Managers	1
D. ERM and Risk Awareness	3
Element 3: COMPLIANCE	
A. Compliance	9
B. The relationship between Compliance and Risk Management	2
C. The relationship between Compliance and Risk Awareness	2
Element 4: IT GRC (Governance, Risk Management and Compliance)	
A. IT GRC	2
B. IT interconnects a company's employees	4
C. IT does reduce the risk to the organisation	4
D. Companies are on the increase to invest on IT GRC	9
Element 5: RISK MANAGEMENT	
A. Why is Risk Management important?	13
Element 6: RISK AWARENESS	
A. Why is risk awareness important?	49

4.4.2 In-depth Qualitative Interviews

In-depth interviews were also undertaken in each of the cases to gather in-depth qualitative data on risk awareness based on a conceptual framework adopted from the literature exploring cognitive, behaviourial, emotional, socio-cultural factors. A sample of two key executives in each organisation from both ADP and the UAE were sampled for in-depth interviews. The interviews provided the opportunity and flexibility to pursue lines of enquiry based on responses received during the course of the interview and gather data reflecting the reality of the interpretations (Bryman and Bell, 2007).

4.4.3 Delphi Technique

The Delphi technique is the third method adopted for this study which is a widely utilised and accepted method for collecting data from participants within their area of expertise (Ritchie et al., 2005). The Delphi technique encompasses a process of rounds of questionnaires continued until a previously decided level of consensus is reached, or until new information is no longer being obtained. In this study two rounds were conducted which was assessed as sufficient given the level of initial consensus among the experts convened.

The technique enjoys extensive credibility with policy makers in which the formalised and traceable methods are valued for strategising and forecasting future scenarios (Grobbelaar, 2007). The opinions of experts are accessed through group communication designed to elicit consensus judgement on specific real-world and long-term issues (Ritchie et al., 2005). This is because the method assumes that experts are better equipped to bring tacit and complex knowledge and experience to bear on research problems than theoretical approaches or extrapolation of data (Cuhls, 2003). It has found to be particularly effective for refining research ideas (Saunders et al., 2009), contributing additional rigour to the research design and outcomes of studies by addressing complex issues difficult to research using more conventional methods (Ritchie et al., 2005). Eto (2003) argues that the technique is particularly suitable for examining research problems such as the blend of human and technical dimensions relevant to topics such as risk awareness that require complex and subjective judgements rather than precise quantitative results.

Moreover the number of experts involved and the ability to partially conceal diverging opinions beneath the main convergence of views is an advantage in being able to identify the primary judgements in relation to risk awareness. The consensus process is systematic and delivered through written means ensuring that problems are considered in a logical manner meaning that the consensus achieved is derived from reasoned opinion and has greater validity than the view of a single individual (Murray and Hammons, 1995). The value of this approach for this research is that the technique provides the scope to explore issues in greater depth and is highly regarded for its ability to access knowledge and expertise otherwise unavailable to the researcher (Ritchie et al., 2005).

Notable limitations include the possibility that a true consensus may not be reached among the experts as consensus-making can be subject to manipulation and bias resulting in less than optimal judgements (Mittroff and Turoff, 1975). To counter this effect and maximise the validity of this method a diverse panel was recruited to reflect differing perspectives and views and the investigation design was rigorously considered in order to ensure clarity and negate the potential for manipulation and bias.

4.5 Data Collection Procedures

Descriptive statistical data and qualitative data was collected from the Abu Dhabi Police Force. The quantitative data was collected in two rounds using a questionnaire. In the first round the questionnaire focused on the three phases of the risk analysis model risk identification, risk analysis and risk mitigation. The questionnaire contained demographic questions and questions to collect data on the organisation and number of employees, and measured the knowledge, behaviour and understanding of employees about risks that may affect their organisation. In the second round, the questionnaire focused on assessing the police force's current knowledge of risk management. It contained multiple choice type questions and collected textual responses to certain questions.

Data collection was undertaken in accordance with the research plan (Appendix A). The research was organised into three work packages: Scoping of IT risk awareness among management and staff in UAE enterprises; modelling the critical elements and the relationship between them and evaluation of the model by experts. Data collection methods were employed to gather data on IT awareness and management to address Objectives 1 and 2: The specific procedures applied for data collection from the case organisations and Delphi expert panel are detailed below.

Abu Dhabi Police

A questionnaire was conducted to compare the practice of the Abu Dhabi Police Force and to use the results in the development of the MERIT IT Systems Risk Awareness model. Several on-site visits to the field case Abu Dhabi Police Force were planned. The first one was to explain the purpose of the research to the Abu Dhabi IT Department management and gain their support. The second visit was to administer the qualitative questionnaire to gauge the current level of knowledge of risk management in the department. The third visit was to evaluate the relevance of the MERIT IT Systems Risk Awareness conceptual model with

consultants, officers and engineers. The fourth visit was to validate the MERIT IT Systems Risk Awareness conceptual model using the Delphi Method.

During a visit on 15 May 2008, 50 staff from the ADP IT department were approached, including the Director of IT and his assistant, seven head sections, the consultant of IT Department and the other fifteen persons.

UAE Organisations

To improve the generalised nature of the principles of risk management and research data, a survey questionnaire was also administered to small (Case8 to Case10), medium (Case5 to Case7) and large (Case1 to Case4) companies in Abu Dhabi. The purpose was to develop statistical descriptions of risk management, perform statistical analysis and to explore the data for meaningful categories. The questionnaire was piloted with a group of colleagues from the Abu Dhabi Police Force and amended according to their feedback. Some questions were unclear to respondents and these were simplified by using non-technical language. Additional questions on managing risk were added to collect management data. The data set was analysed by using the cluster analysis procedure.

4.6 Data Analysis

Both qualitative and quantitative data analysis techniques were applied. Content analysis to organise and interpret qualitative data from the surveys. While univariate and multivariate statistical techniques were employed to analyse quantitative data from the surveys and Delphi panel. This data is analysed using statistical tests such descriptive statistics, K-means analysis of clusters, Dendrograms using hierarchical clustering and response analysis of Delphi experts' panel. The data was analysed using the statistical software package SPSS. Qualitative data enabled discovery of significant categories of importance from data. This was done by identifying themes by coding the data based on reading the literature. This resulted in producing qualitative findings. The elements of the MERIT IT Risk Awareness model were improved by using these findings.

Cluster analysis is a major data analysis tool for classifying large amounts of observed data into more manageable and meaningful groupings. In this exploratory activity the definitions of clusters and which elements belong to them are not previously known and emerge through analysis of the data (Bickman et al., 2008). The value of cluster analysis lies in the ability to

quickly and efficiently identify themes within the data that form the foundation for further analysis while also allowing the examination of a full range of inter-relationships between variables. This is achievable through cluster analysis as groupings are generally based on combinations of independent variables which maximise the similarity of data elements within that cluster while increasing dissimilarity between different clusters which are at first unknown (Alasuutari et al., 2008). This statistical technique is applied as the basis for discovery to provide and inform the classification of risk awareness from the quantitative data gathered.

Two clustering methods were used (a) the basic Clustering procedure and (b) the Hierarchical Clustering Method. The first method is useful for a large number of respondents, for which it helps by putting a set of observations into subsets (called clusters), so that observations in the same cluster are similar in some sense. The method is unstructured or 'unsupervised learning'. It brings hidden values into light by clustering them and highlights data which identifies groups that behave similarly or show similar characteristics. Hierarchical clustering method is known for its good performance with small respondents, less than hundred participants. Hierarchical clustering is simpler to use and it can be either agglomerative or divisive. Both methods were implemented on SPSS. Hierarchical clustering method was used to produce cluster trees or dendograms to identify the classifications.

Qualitative data was analysed using a content analysis approach. According to Yin (1994) qualitative data analysis can be understood in terms of examination, categorisation, tabulation, and other methods which synthesise evidence to answer the research questions. For this study this involves the identification of principal variables and theories in the field of risk awareness. Having achieved this a thematic analysis procedure suggested by Cresswell (2009) was utilised to form a systematic underlying methodology for the analysis to reinforce research validity and reliability of the qualitative research. Initial stages involved the organisation of the data entailing transcription of the interviews which provides a structured and usable format for analysis (Seale et al., 2007). Following preparation of the data for analysis the next step is the coding process which is one of the most significant parts of the analysis process (Creswell, 2009).

The data from the case interviews was analysed using an iterative process involving clustering and organising the evidence based on key words identified in relation to theories of

risk awareness and its associated concepts so that patterns could be discerned. Utilising this method it was possible both to determine and make sense of the risk awareness activities of the case organisation and its managers and to examine how the evidence aligned with theory. As part of this phase Cresswell (2009) underlines two main types of coding strategy firstly involving more content-based coding. These codes are generally straightforward intuitive codes, of conceptual interest or addressing wider theoretical points of the research. Setting and contextual codes form the basis for a second type of coding which generally focus on participant perspectives, their views and outlook in relation to other people and the material world, relationship and social structure, or activity. As the goal of this stage is to identify the relevant theories and variables highlighted in the literature an analogous coding procedure is utilised to the meta-analysis of Van Wijk et al. (2008) of the organisational knowledge transfer literature.

After preparing the data for analysis an initial reading of the text was conducted in order to note items of interest, major issues and any emerging themes and which supported initial impressions of the various topics embedded in the data (Guest et al., 2011). A second reading involved a more in-depth analysis in which the text was examined line by line, and utilising open coding methods related topic items were organised and categorised into initial themes. These were purposely kept simple in order to allow the flexibility for modification and development during further re-reading of the data (Boyatzis, 1998). The text was then re-examined in a second process of axial coding during which every part of the data was now considered and categorised explicitly in terms of the themes identified. This process is considered vital and was performed attentively in order to ensure that the potential relevance of data to any theme was not overlooked through the human tendency for selectivity and bias (Guest et al., 2011). The final stage involved construction of the conclusive form of each theme including re-examination of definition and supporting data focusing on the underlying meaning of each theme (Boyatzis, 1998).

4.7 Validity and Reliability

External validity or transferability is related to the extent to which the data can be generalised and how far the findings are applicable in other contexts or among other groups (Lincoln and Guba, 1985). According to Lincoln and Guba (1985) this process can be supported through the provision of "thick" descriptions of the data and findings to provide a platform for the reader to evaluate the potential application of the results in different contexts. The

employment of an accepted and systematic methodology for the analysis of the data further enhances the rigour of analysis implying greater validity of the results. The final step is to ensure that the data is presented in such a way in the discussion of the research findings that an evidential logic is apparent from the raw evidence exampled through to the final themes. Considerations of reliability and dependability involve exploring the stability of the data in terms of how replicable the results would be if repeated in a similar setting with similar participants (Creswell and Plano-Clark, 2007, Lincoln and Guba, 1985). There is a close relationship between credibility and dependability and ensuring the former may to a great extent promote the latter. Shenton (2004) argues that to support reliability and dependability overlapping methods which are encompassed by mixed methods research designs are encouraged. This is in conjunction with an in-depth description of the research process which this chapter is seeking to provide.

Furthermore, a mixed method approach enhances the validity of the research findings Triangulation is a significant aspect within the implementation of mixed methods research as it helps to enhance the overall trustworthiness of qualitative methods (Denzin and Licolm, 1994). Trustworthiness, a significant aspect of the evaluation of qualitative research is constituted of four main research criteria: credibility (internal validity); transferability (external validity); dependability (reliability), and conformability (objectivity). Furthermore the triangulation of data collected using different methods and sources to examine the same phenomenon means that the problem can be elaborated in greater depth and corroborated (Bryman, 2006). Another advantage is the limitation of researcher and methodological bias which supports greater generalisability of the findings (Decrop, 1999). Data and methodological triangulation can therefore enhance the credibility of the findings.

The competency of the researcher can impact significantly on the validity and reliability of the study either through researcher bias or in undermining the research design process (Saunders et al., 2009). To counter such issues appropriate training was undertaken in relation to all stages of the research process including an accredited a four month postgraduate course in Research Methods for Technology. In addition, attendance on a Risk Awareness Workshop provided a sound basis for identifying and mitigating risk which was applied to the research process.

4.8 Sampling Strategy

The sampling for this research is based on a purposeful case strategy. While both quantitative and qualitative data has been gathered the choice of this strategy was influenced by the decision to gather data across multiple organisations according to a predefined criteria. This strategy allows for the judgement of the researcher to inform the sampling of case organisations and the experts. While sampling quota is desirable it was not a strict requirement. Further, given the case study approach adopted and the multiple methods of data collection this approach allowed flexibility for selection samples to meet the purposes of the research objectives. Within the organisations the sampling strategy for the quantitative surveys was on convenience sampling of a cross-section of the workforce.

A significant element of conducting a Delphi study is the selection of the panel of experts. Dalley et al., (1972) shows that increased group size leads to greater reliability of responses with reliability peaking at a group size of nine, while Debecq et al., (1975) recommend using the minimally sufficient number of participants. Using these suggestions a panel size of six was convened for this study. The selection of the participants was driven by considerations of diversity and heterogeneity of perspective and role in relation to risk awareness in order to enhance validity (Linstone and Turoff, 1975). Experts were therefore selected to be representative of sector, or position and roles (IT/non-IT).

4.9 Ethical Considerations

Ethical principles are fundamental to the conduct of every stage of the research study and are vital for the protection of both researcher and participants. Ethical standards safeguard the rights and the wellbeing of participants and are designed to reduce the risk of mental and physical harm, danger or discomfort which may arise from research processes (Belk, 2007). From the researcher perspective adherence to ethical guidelines protects the right to conduct legitimate studies in addition to preserving the reputation of academic institutions or sponsoring bodies and avoiding claims of negligence or unethical practices (CCCU, 2006). The main ethical principles involve the fidelity, justice, and veracity of the researcher, the autonomy, confidentiality and non-harm of participants, and the wider benefit of the research. This research was undertaken following in-depth consideration of how this research may advantage participants and have wider societal benefit. In promoting increased understanding

of risk management and the role of risk awareness this study provides an important contribution towards knowledge for the safety and protection of enterprises from risk particularly in the under-researched context of UAE organisations. Moreover the outcomes of the study provide in-depth insight and will have significant impact on the practices of the ADP which in turn may lead to increased public service effectiveness.

The conduct of this investigation has conformed to the key principles underlying ethical research of which one of the most prominent is to ensure that the risk of harm to either participant or researcher is minimised (Saunders et al., 2009). Accordingly substantial prior consideration has been given to research design and processes to reduce any inherent risk of harm and to safeguard the rights of participants. One significant risk which has been recognised and scrutinised links to the principle of autonomy for participants. This requires that the right of individuals to make their own decisions is acknowledged and respected and forms the foundation upon which the entitlement to free and informed consent is based (Cohen et al., 2013). Adhering to three major elements of informed consent this study provided accurate, truthful and sufficient information to allow comprehension of the nature of the research, its purpose and the processes and procedures followed in addition to detailing any potential risks or benefits. Participants´ volition was fully supported through the voluntary nature of the study of which participants were informed of their right to withdraw at any point in the research (CCCU, 2006).

The research was conducted in accordance with the ethical research policies and procedures of the University of Gloucester. Further, during the course of this research steps were also taken to avoid harm to participants through the negligent exposure of information which compromises their entitlement to privacy and confidentiality (Cohen et al., 2013). The principle of the protection of privacy and confidentiality is essential to ensure that freely given information does not impact the welfare of participants (CCCU, 2006) and was safeguarded in this study through protection of access, control and dissemination of personal identifying details.

This study further acknowledged that ethically it was important to build a trusting relationship with participants without which the fidelity and quality of the data can be compromised (Saunders et al., 2009). Besides ensuring that participants were fully informed of their rights trust-building extended to engaging with any concerns or issues the participants

may have had. Further the wellbeing of participants was continually monitored during the participant elements of the research process and considerable reflection was focused on ensuring justice and fairness, including making certain that all participants were fairly and equally treated and selection procedures were impartial.

The researcher is a Senior Police Officer in the UAE police force on sabbatical to research risk management. His position in the police force may be a cause for concern amongst some participants. However, a strict code of conduct was formulated for collecting data from the participants. To resolve ethical issues involved in the study, all participants were volunteers and were provided with a clause of confidentiality. This ensured that the identity of the participants was kept confidential. In this regard, a consent agreement to this effect was provided to the participants. They were also informed about how the information provided by them would be used in the study. Only relevant information would be collected and used for the purpose of the research.

4.10 Conclusion

This study has introduced a robust research design employing various different methods to collect both quantitative and qualitative data to answer the research question. A realist philosophical approach was adopted aligning with a mixed methods research design viewed as critical for fully investigating the multi-layered and multi-dimensional nature of risk awareness. Utilising a case study strategy to investigate IT risk awareness within both Abu Dhabi Police and UAE organisations a structured questionnaire, in-depth interviews and Delphi technique were applied to gather the data to inform the conceptual model of risk awareness. The validity and reliability of the study findings were supported and enhanced by the utilisation of mutually reinforcing mixed methods and triangulation of the data in conjunction with a systematic and accepted methodology for data analysis.

Chapter 5 Police Forces and UAE Organisation Studies

5.1 Introduction

This chapter presents the results of two quantitative surveys and in-depth interviews investigating risk management and awareness in the Abu Dhabi Police and cross-sector UAE organisations. The results from in-depth interviews from a selected sample of the ADP and UAE organisations are also presented. This chapter is divided into three main sections. Section 5.2 presents the findings from the study with police forces and shows how police force managers, officers, technicians, experts and their employees understand risks facing the organisation and perceptions in relation to force development and implementation of risk management. Section 5.3 presents the results of the survey of UAE organisations to investigate the conceptual understanding gained from the literature review. It aimed to investigate whether risk awareness, the unit of analysis obtained from the literature review, has an impact on risk management. Section 5.4 presents the results of qualitative data obtained from in-depth interviews from samples of key personnel in those organisations.

5.2 Abu Dhabi Police Study

5.2.1 Introduction

To form an initial understanding of risk management knowledge and practice in the Abu Dhabi Police Force IT Department, data was collected to identify significant categories. The questions sought to probe the participants' understanding of the importance of defining risk in order to plan for it and prevent the escalation of problems. It also established the level of knowledge of participants as to how much of a threat they faced and whether this risk would

affect the objectives of the organisation if it occurred. Three categories of personnel were surveyed of engineers, technicians and managers. This included managers of the: IT Department, Support Technicians, Security Information, Communications, Security Systems, Deputy of IT and Experts.

5.2.2 Result of Abu Dhabi Police Survey (Information Technical Department (IT)

From the first round of data shown in Table 4, diverse knowledge levels of risk management among the Abu Dhabi Police Force participants is revealed. Only 9% of the respondents could accurately name 'risk' as an occurrence of harmful effect on the organisation and only 8% of the respondents could accurately name accidental disclosure of data as an IT systems risk. Detailed knowledge of risk management was weak; however 42% respondents were aware that risk management requires identification of threats and corrective actions to mitigate it. Approximately 70% respondents were aware that risk to IT systems composed human risk, security risk, technological risk and system failure.

Table 4 Levels of Risk Management Knowledge in Abu Dhabi Police Force in 2008

Category	**Per Cent**
Risk	9
Accidental disclosure of data	8
Identification of threats and corrective action	42

In Table 5, nearly 70% of the respondents acknowledged that skills, cultural awareness, appreciation of the importance of risk management and communication were critical aspects of 'risk awareness'. The result for training on risk management was evenly divided, with 58% of respondents reporting receiving training and 42% confirming that they had not received any training. More than two thirds of employees believed they were equipped with skills and have authority to take autonomous action to mitigate risk without obtaining prior approval

from their line managers. A third of the respondents believed that external or internal consultants have the responsibility to identify risk whereas less than 25% perceived that it is each employee's responsibility to assess organisational and IT systems risk.

Table 5 Risk Awareness in Abu Dhabi Police Force in 2008

Category	**Per Cent**
Awareness of composition of IT risk: human risk, security risk, technological risk and system failure	70
Risk management training	58
No risk management training	42
Confident in their skills to take action to mitigate risk	66
Consultants and Internal Experts Task to identify risk	33
Individual's responsibility to assess Organisational risk	25

In terms of risk awareness, a third of the respondents did not believe that the IT department had a risk management plan. This is a notable result as an indication of the degree of risk awareness and communication as it is public knowledge that the Abu Dhabi Police force has such a plan but it is evident from this result that it is not well communicated and implemented. Substantiating this evidence, a further, 67% per cent of respondents state that the IT department does not perform regular risk assessment and 17% state that AD police as a single entity does not have a risk register. A further 42% of respondents view the increase in the IT system risk for AD police over the last five years as a negative sign for existing risk awareness and management mechanisms. All the respondents (100%) believe that it is the IT department's responsibility to deal with risk and related risk awareness processes.

Table 6 IT Systems Risk Awareness

Category	Per Cent
Belief that IT department has no Risk Management plan	33
No regular risk assessment	67
No risk register	17
Increase in IT systems risk is negative	42
IT department is responsible to risk management	100

5.2.3 Summary of Results

The results show that a diverse level of knowledge in relation to risk awareness and management is evidenced in the Abu Dhabi Police Force. Gaps in awareness were evidenced as detailed knowledge of risk management was weak and a large minority was not aware of the existence of IT risk management plans. In contrast awareness of the different types of risk was high in addition to knowledge of critical aspects of risk awareness such as skills and cultural awareness. However a key result highlights that all of the sample believe that it is the sole responsibility of the IT department to address risk and related risk awareness processes, reinforced by the majority view that it is not each employee's responsibility to assess organisational and IT systems risk. In terms of organisational practices to support risk awareness the results indicated a low level of implementation. The provision of training was far from universal while the performance of risk assessment by the IT department was perceived as inconsistent and highly irregular.

5.3 UAE Organisations Study

5.3.1 Introduction

The study surveyed a number of UAE organisations in other sectors to collect data on current practices focused on compliance of risk awareness and management and the lessons that can be applied within the AD Police. The purpose was to develop statistical descriptions of risk management, perform statistical analysis and to explore the data for meaningful categories.

5.3.2 *K-means* Analysis

The survey data was analysed using the *k*-means method of clustering techniques. Mathematical clustering is used to discover similarities and differences in datasets. The *k*-means clustering method was used because it provided meaningful groupings with similar parameters, or features. The aim was to identify similarities in proved Risk Management practises from different organisations.

The *K-mean*s analysis is generated by stating the relevant cases to use and the question values to cluster. SPSS software then generates various statistical tables, including the *K-mean*s for each cluster. K-means analysis allows one to cluster or to partition the number of observation into clusters wherein each observation is considered in a cluster with the nearest mean value. Thus, K –means analysis allows the separation of data according to their mean values in different cells. In this study, measures are clusters for each hypothesised variable proposed as a factor of risk awareness in the MERIT risk model in chapter three.

5.3.3 Hierarchical Cluster Analysis using Dendrograms

The questionnaire results of the most important questions are discussed in this section using histograms plotted from responses received for each question. Each graph indicates a significant aspect in relation to organisational and employee understanding of risk awareness and management. Questions were framed for each element to understand the relation between the element and risk awareness and how they affect the other components.

Element 1: GOVERNANCE

Figure 6 shows that seven of the companies scored highly in demonstrating knowledge of risk awareness. This result implies that these companies have a well communicated policy or guidelines in risk management. One company indicated a complete lack of awareness which, in contrast, suggests a lack of policy and guidelines. Two of the companies were “probably aware” which means that potentially they have a policy or guidelines in risk management but were lacking in effective communication.

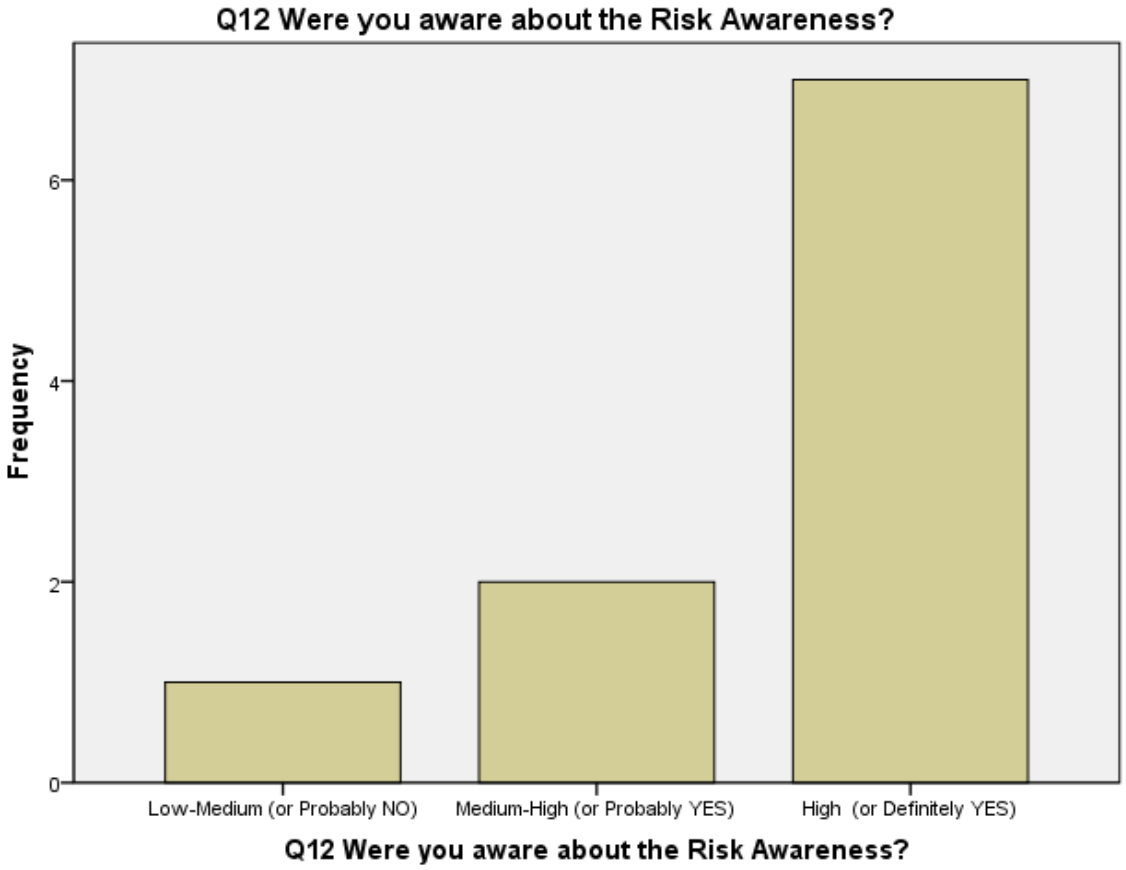

Figure 6 UAE 10 Companies Response

Figure 7 shows cases are listed along the left vertical axis (Case1 to Case10). The horizontal axis is the distance between clusters when they are joined. It shows six clusters (C), the closest one is C2 and C3. The inference from this is that large companies are more aware of risk and therefore take action to counter it.

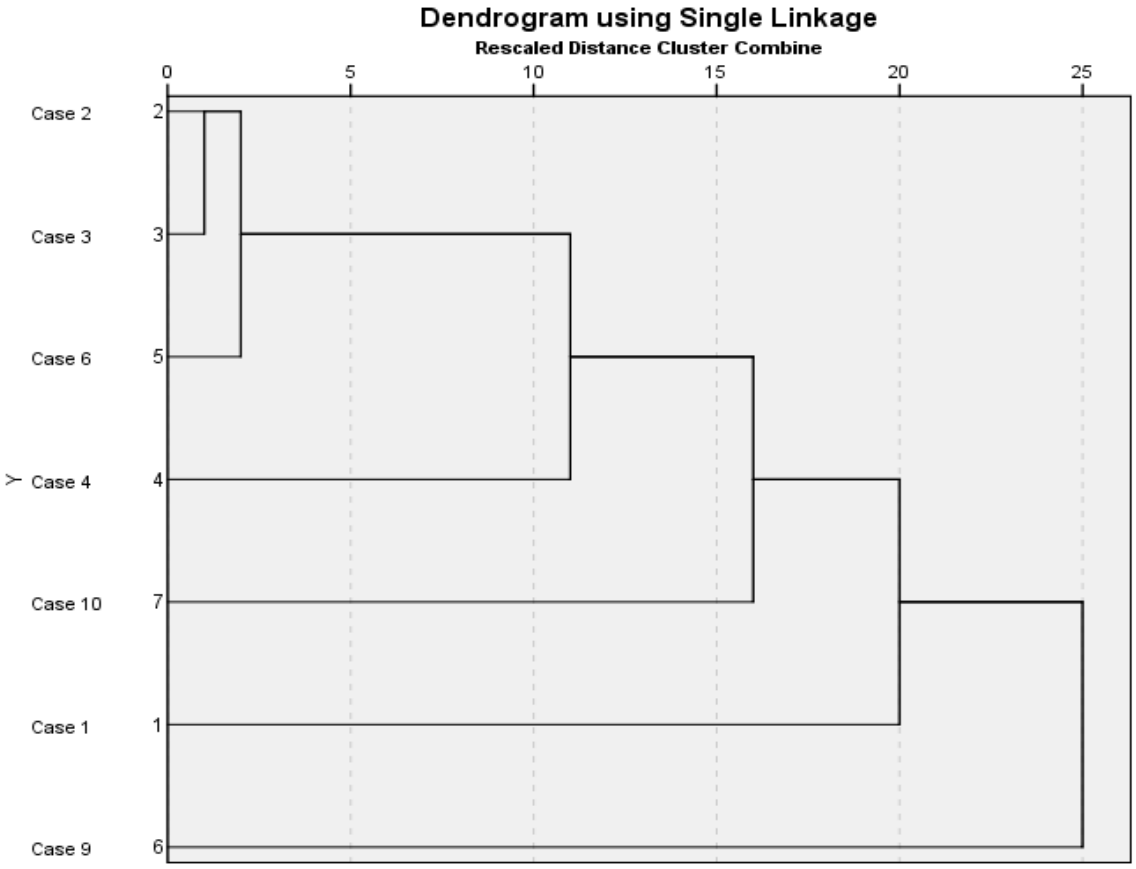

Figure 7 Governance Cluster analysis using Dendrogram

Element 2: ENTERPRISE

Figure 8 shows 7 clusters (C) the closest of which is C2 and C7 demonstrating that the larger to medium sized organisation perceived that risk awareness will lead the enterprise to reduce the risk that can impact their business. The finding shows that smaller organisations are less active in this area.

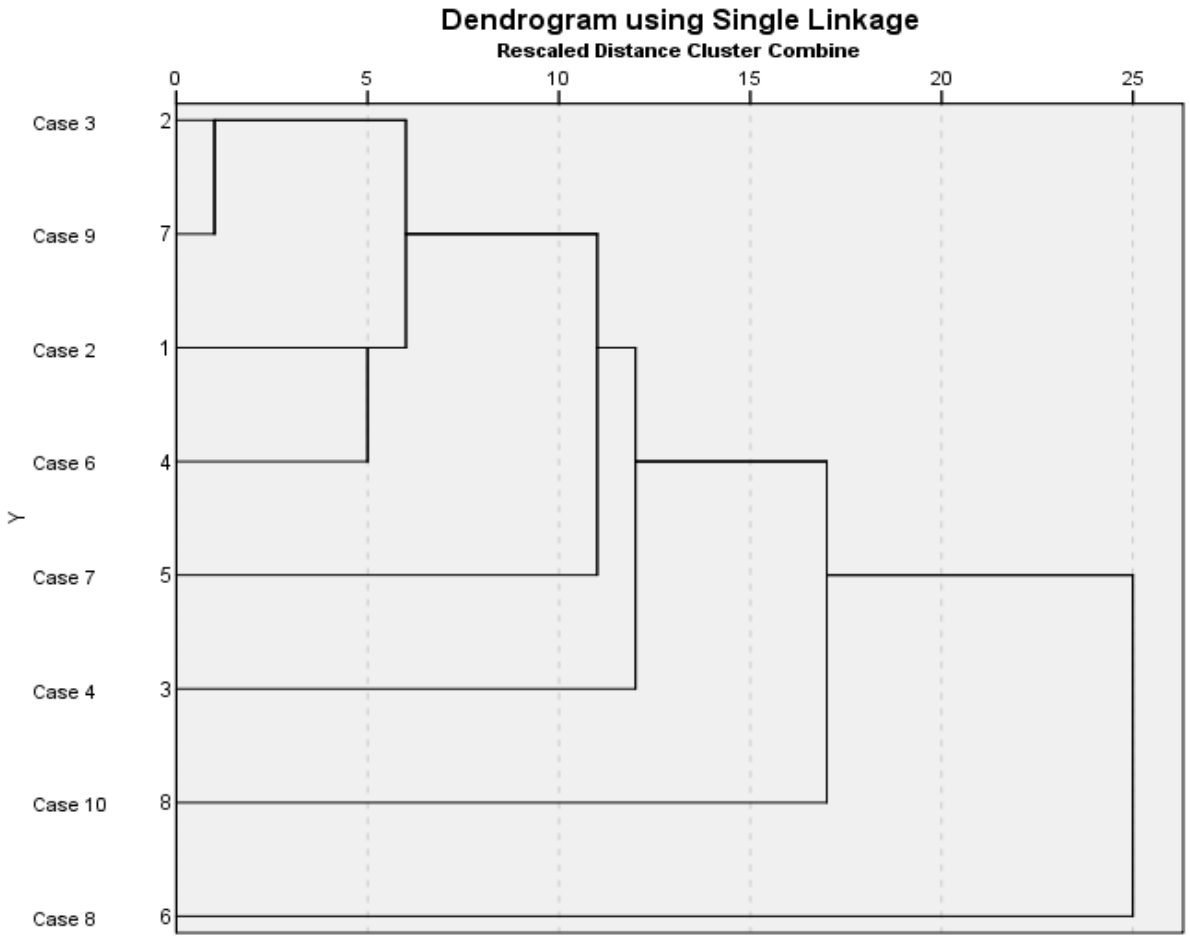

Figure 8 Enterprise Cluster analysis using Dendrogram

Element 3: COMPLIANCE

When asked whether risk awareness will lead to compliance Figure 9 shows 8 clusters(C) the closest of which is C4 and C8. This indicates that medium and small companies agreed that improved compliance of risk awareness will reduce the risk that can impact their business.

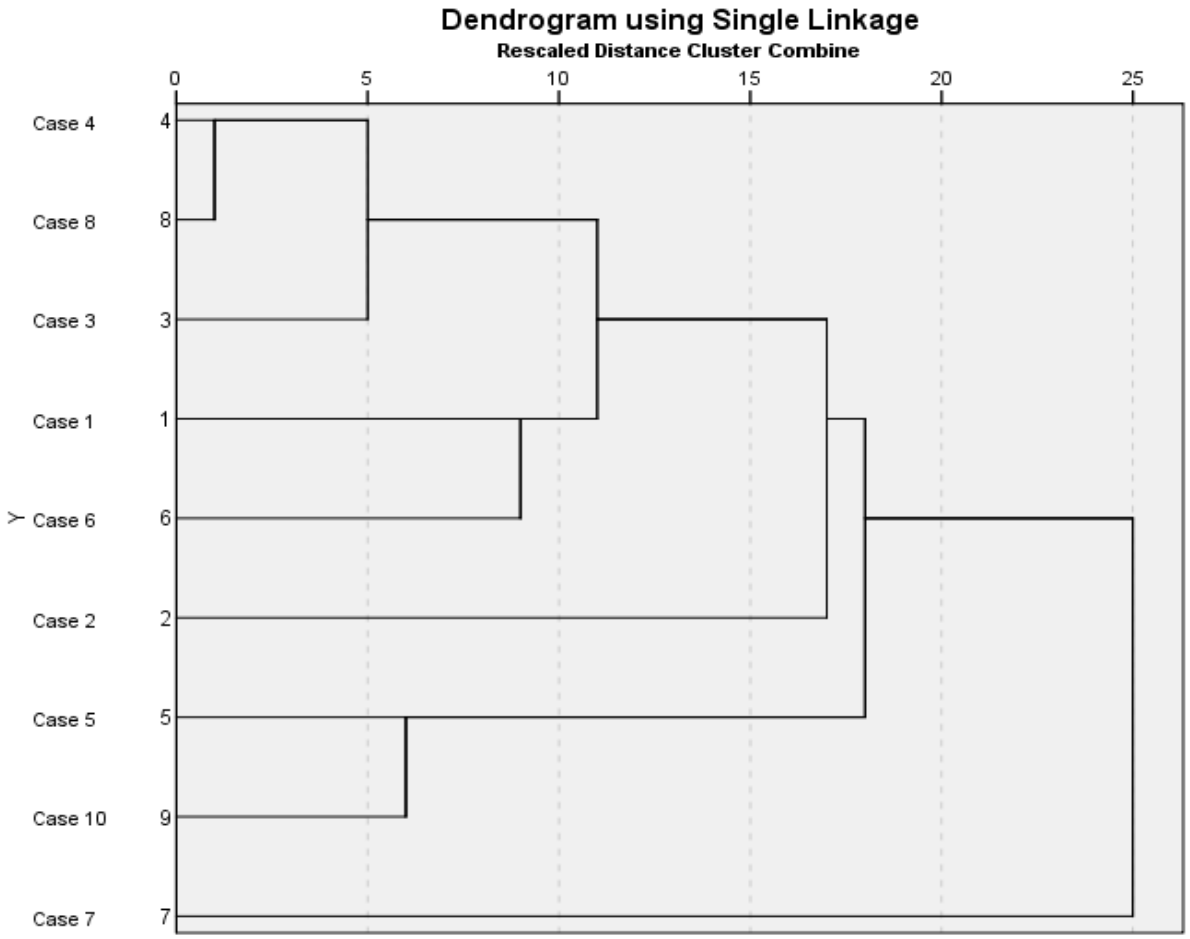

Figure 9 Compliance Cluster analysis using Dendrogram

Element 4: IT GRC

Limited agreement was evidenced amongst large and medium companies that IT can be used to control the workflows of audit and risk management, as shown by Figure 10 in which of the 8 clusters(C) C1 and C6 are significantly the closest. The results suggest uneven understanding of the significant role of IT in risk management and other elements.

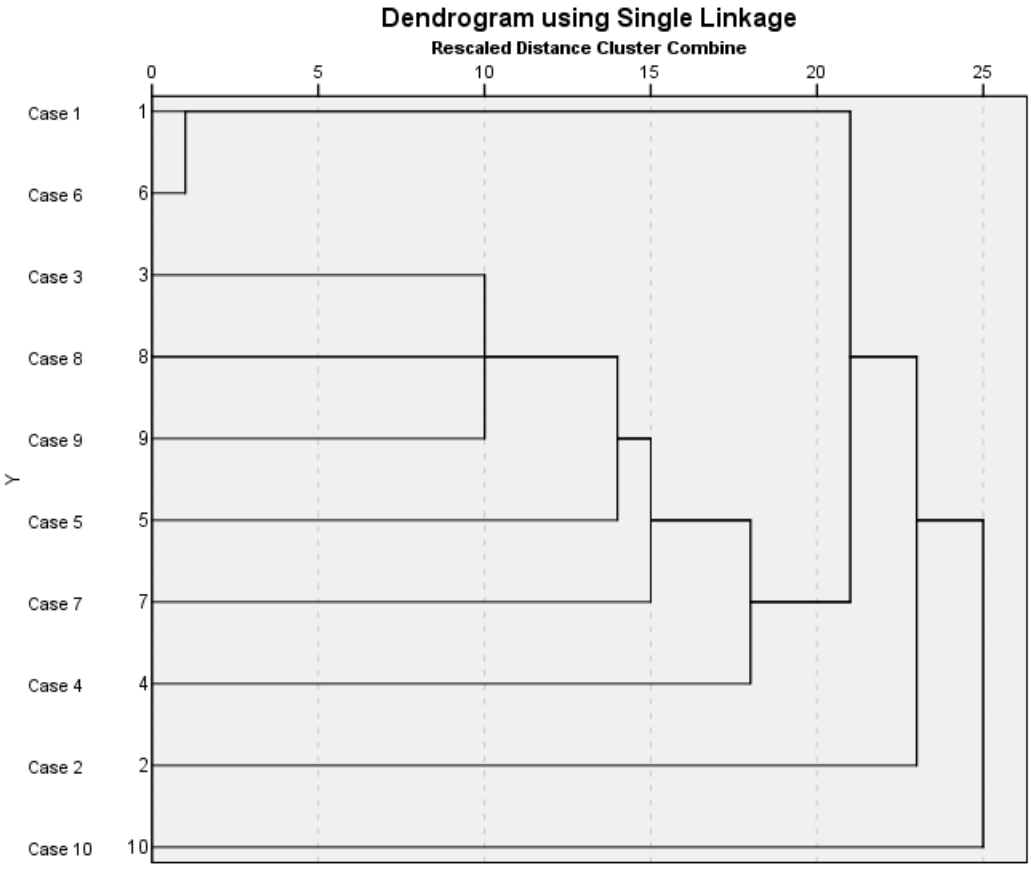

Figure 10 ITGRC Cluster analysis using Dendrogram

Element 5: RISK MANAGEMENT

In relation to the extent that Risk Management was perceived to reduce the effect of IT risk Figure 11 shows 6 clusters(C), the closest one is C3 and C7. Whilst only two have agreed, this is clearly a potential point to develop for the model.

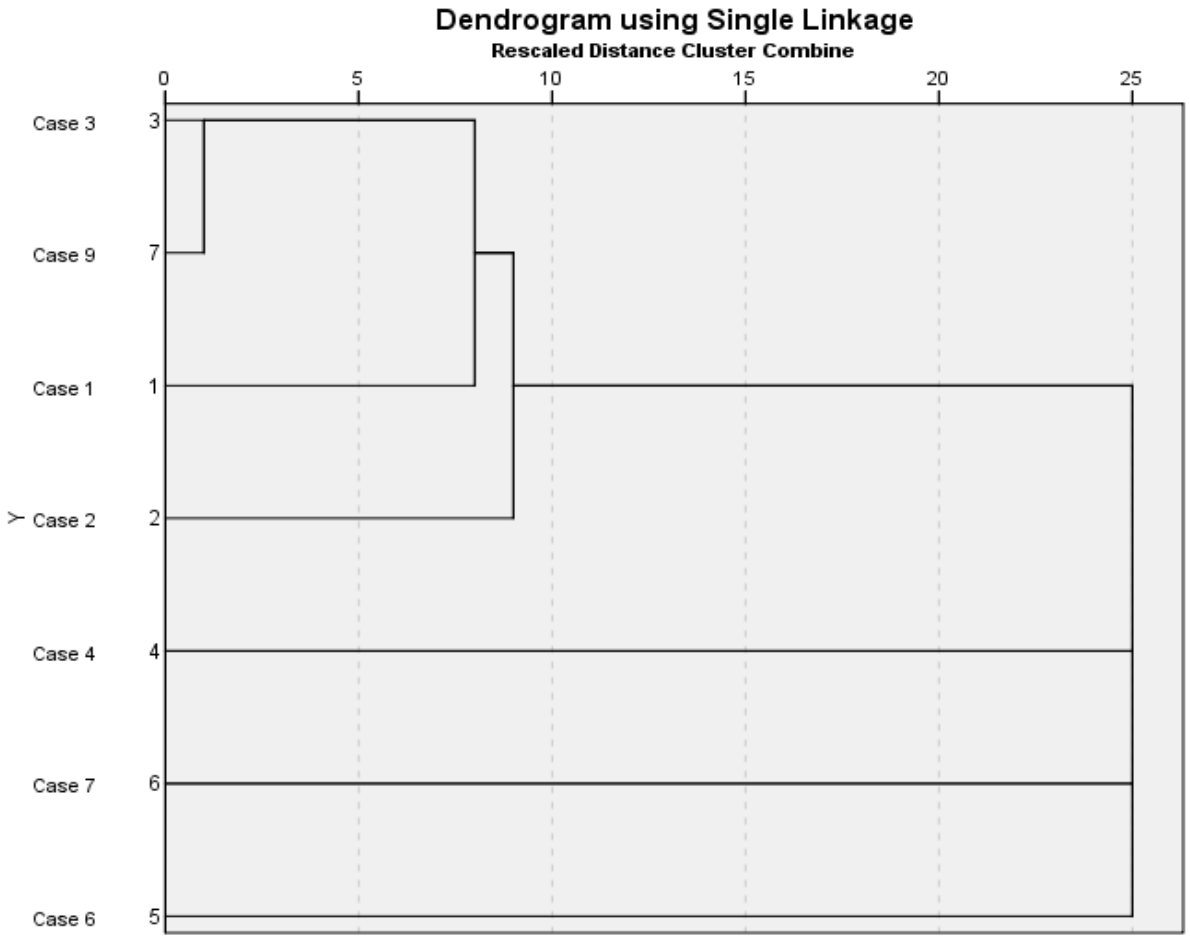

Figure 11 Risk Management Cluster analysis using Dendrogram

Element 6: RISK AWARENESS

The results indicate significant consensus that risk awareness is important and all need to be clear on what threats they face as shown in Figure 12. This highlights 4 clusters(C) indicating closer cluster agreement amongst C1, 4, 5 and 6.

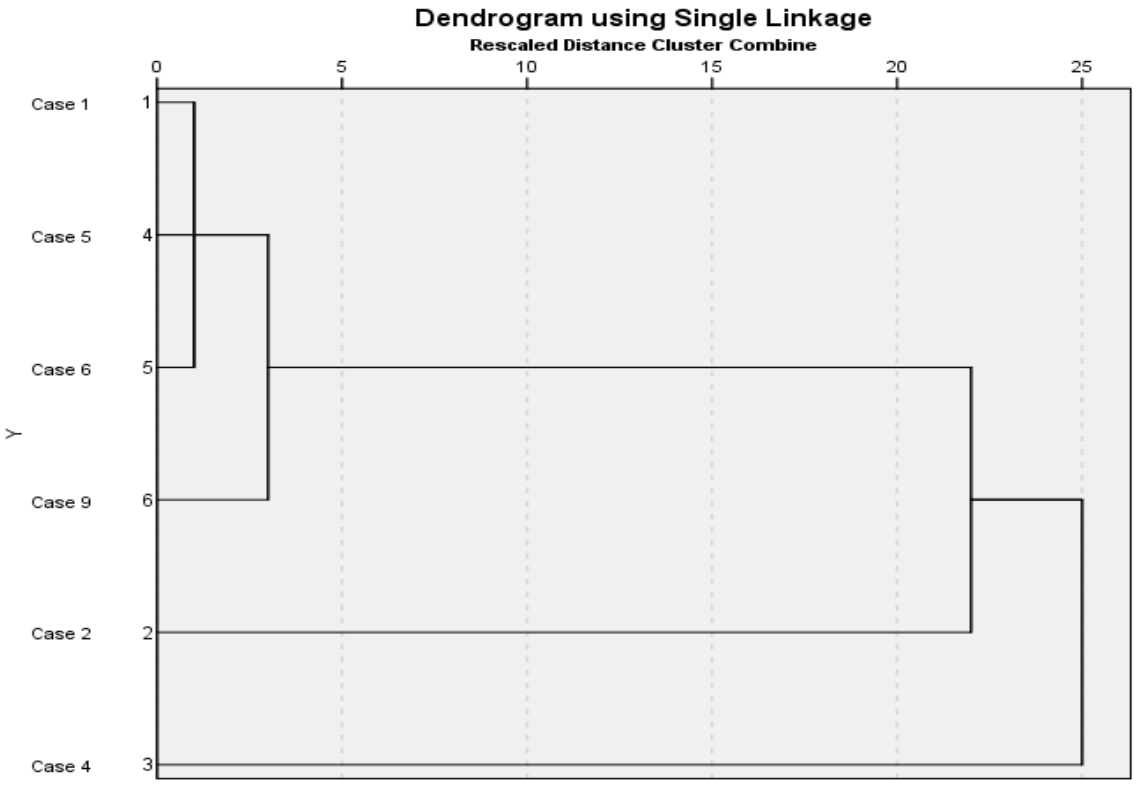

Figure 12 Risk Awareness Cluster analysis using Dendrogram

5.3.4 Summary of Results

The results of this survey of UAE organisations indicate that practice of risk management in these organisations is more developed than that of the AD Police. A high level of knowledge of risk awareness is evidenced among the majority of companies. Moreover the consensus indicated that risk awareness is perceived as important for clarity on potential threats the organisation may face. However the findings emphasise that larger companies are more aware of risk than smaller and generally take measures to counter it. Both larger and medium sized organisations emphasised the significance of risk awareness for reducing the risk that can impact their business. Further medium and small companies agreed that improved compliance in relation to risk awareness can reduce risk. In conclusion the results from the UAE case organisations help to form the current and collective understanding of risk management practices in the UAE. These organisations are significant and representative in both size and sector. By selecting the best policy from these companies, lessons can be implemented within a public body such as a police force. In turn, these lessons support the development of a risk awareness conceptual model.

5.4 Qualitative Interviews

5.4.1 Introduction

In-depth interviews were also undertaken in each of the cases to gather in-depth qualitative data on risk awareness based on a conceptual framework adopted from the literature exploring the MERIT model and underlying cognitive, behaviourial, emotional, and socio-cultural factors. The results present a number of findings contributing towards conceptualisation of the MERIT model and IT risk awareness.

5.4.2 MERIT Model

The results of the qualitative interviews supported the usefulness and importance of the MERIT model and its components for providing a robust conceptual framework for applying and evaluating risk awareness. The consensus from respondents emphasised that each element of Governance, Compliance, Enterprise, IT GRC and Risk Management provide integral, iterative and critical perspectives for considering risk awareness within organisations.

In particular governance was accorded substantial significance within the model as a key element enabling and supporting other components. One respondent remarked: *"Governance is important for risk awareness because it represents a mechanism through which risk awareness can be embedded."* This highlights the role of governance as a driver for enterprise and cultural responses towards risk awareness. Another stated:
"Governance is vital to ensure that the issues are visible and effectively monitored. When the security context changes then governance processes can promote risk awareness and at the same time can be supported by risk awareness."

Emphasis was also placed on the role of governance in the facilitation of accountability and individual responsibility in risk awareness and management: *"You need effectiveness in governance to ensure good accountability and to make sure that the processes are visible to everyone."*

Another respondent stated: "*Governance is important because if you promote shared decision-making and ownership and collaboration then you raise awareness. At the same time you counter the individual bias because you create a supportive environment. The*

leadership aspect is important because you empower people to take chances in terms of getting to grips with an issue and developing heightened awareness. At the same time effective leadership, coaching and mentoring can promote knowledge exchange and transfer which in turn can maximise awareness."

However one respondent highlighted that risk awareness is frequently not perceived by employees as a collective responsibility: *"In some cases the awareness of risk is undermined when people consider the problem belongs to another department or person".* The last point emphasises the importance of governance and accountability to risk awareness.

The respondents further placed particular emphasis on the importance of enterprise-wide dimensions for promoting risk awareness. One participant commented that: *"This has to be enterprise-wide so that you promote co-operation and collaboration and people working to shared goals."*

Another stated: *"However this needs to be enterprise-wide because such a heightened level of awareness cannot be achieved based on small number of individuals but through a combined effort."*

The evidence from respondents in the sample suggests that awareness is undermined because of the existence of certain silos in the organisation which inhibits knowledge sharing about issues and can therefore impact enterprise-wide understanding of issues.

However one respondent expressed views over the danger of implementing risk awareness programmes and structured programmes for raising risk awareness which in their experience can have unintended consequences: *"The problem is that risk awareness programs become an additional activity or checklist. My experience is that we need to build in processes into the work flows."*

Another respondent commented that in order to promote effective risk management it is necessary to maintain a high level of awareness. *"We have awareness of IT security but sometimes this is only a vague sense. "*

5.4.3 Elements of Risk Awareness

Respondents were also questioned in relation to their perspective on the underlying and integral elements of risk awareness including cognitive and subjective processes. A consensus among participants emphasised the importance of comprehension of a range of different types of IT risk and their sources for an effective level of risk awareness. However respondents noted that types of risks can be perceived in many different ways underlining complexity in understanding the types of risk. The majority further underlined that in the IT context risk was dynamically changing, expanding and consistently growing in diversity which presents significant challenges for identifying different types of risks. According to several participants this indicated the need for training on demand to continually update organisation and individual level risk awareness. However; most participants expressed the view that this was insufficient in their organisation.

The findings however point to issues and challenges in maintaining relevant and up to date knowledge on the diverse and dynamically-changing IT threat environment. One respondent remarked:
"It is very challenging and complex when the environment is constantly changing and therefore you need some method to understand whether the level of awareness is satisfactory".

Another commented: *"Sometimes this can be due to rapidly changing environment because IT security risks are constantly evolving and this process needs to change to keep pace."*

In particular the majority of respondents also indicated the view that IT risk awareness depends on an understanding of common and critical IT risks with the majority stating that this was an area of weakness in their organisation. This was viewed as important for focusing the effectiveness of risk awareness efforts in essential security areas. However several participants claimed a lack of systematic and continuous identification and comprehension of critical risks through enterprise-wide risk management and governance structures and failure to quantify the potential impacts. This resulted in perceived negative impacts on levels of risk awareness. One respondent remarked:

"For instance we have a high level of awareness of the existence of digital security and digital crime and that there are many critical risks. However for many this awareness impedes in many ways because of their knowledge of the specific risks or even the severity of certain risks."

A robust consensus was evidenced on the need for diverse and flexible sources of knowledge to inform risk awareness as the participants expressed the benefits for forming a comprehensive view of existing and potential or future risks. Several participants pointed to knowledge frequently arising from the external environment and emphasis was additionally placed on mechanisms which promoted an increase in external knowledge flows and knowledge sharing across different levels, functions and organisations in order to maximise risk awareness. However the majority stressed knowledge diversity as a weak factor within their organisations particularly in relation to obtaining external knowledge.

Some respondents noted experiencing higher levels of risk awareness on issues where they experienced greater and regular interaction with other parts of the organisation. One respondent noted:
"*I feel more confident and secure in my awareness of issues when I am interacting with employees outside my department. I gain a better sense of the range of risks and their severity when I have the opportunity to discuss and contrast outside of department".*

Another respondent state: *"I feel better able to perceive new risks or areas of risks when I am able to discuss them with others."*

Moreover there appears equal weight placed on informal opportunities for learning and information sharing as there are for formal. According to one respondent *"most of my awareness comes from informal discussions I have with my colleagues".* This emphasises the role of informal learning and social networks in raising awareness of issues. The result also places emphasis on external connections for raising awareness as one respondent notes the importance of social media: *"The information we receive from social media channels provides a rich source of information and allows us to better understand, prioritise and perceive risks"*.

Another participant remarked: *"These linkages should not only exist internally but with external stakeholders. Risk awareness can be maximised by using social media more effectively to connect and engage with the public. Information from the public can raise awareness about a wide range of issues. Examining channels for communications and engagement can form part of a tool in raising risk awareness."*

The respondents further highlighted that their dynamic operating environment involving consistently changing risks significantly emphasised detection and understanding of new and novel risk and threat sources as an effective component of risk awareness. However the consensus view pointed to significant weaknesses in risk awareness practices in relation to detecting novel risks. Several participants noted a lack of proactive activity or processes to continuously update knowledge and as a result some participants felt that this undermined overall risk awareness and increased vulnerability. In contrast familiarity with risks was noted by the majority of participants to lower the risk perceptions of individual users and the need to consistently emphasise the potential dangers in known risks was highlighted.

The participants placed great emphasis on understanding of the different cognitive processes informing risk awareness. The view was generally taken that two essential cognitive components comprise the ability to detect hazards in conjunction with being able to subjectively evaluate the potential consequences or risks that these hazards pose. This aspect was highlighted by the majority as frequently failing to be considered within risk awareness strategies however perception of risk without the cognitive capacity or information to evaluate these appropriately was held to be insufficient for complete risk awareness.

The view of the majority of respondents indicated the greater need for a presence of mind and common sense in relation to consistent awareness of IT risk. This was expressed in terms of being aware and engaged in the present and noticing new elements in the environment which may pose a risk. In particular it was noted that this aspect impacted on risk management performance across the enterprise on a critical as well as a routine daily level. The need was felt for this element as a critical part of risk awareness as the consensus indicated the impossibility of prescribing behaviour for every circumstance or eventuality. A further reason given was constantly changing risk. One respondent remarked:

"I think there is a lack of awareness in relation to understanding what actions can be undertaken to mitigate risk. Perceiving IT risks is vital and then means people have to be in closely in touch with the environment and receive regular flows of information and indicators and signal which can raise their awareness."

Respondents also underlined the significance of enterprise risk culture and the influence of collective norms, values, and knowledge as fundamental socio-cultural factors within risk awareness. The majority signaled that demonstrably shared risk values and behaviours could potentially heighten risk awareness through acting on basic assumptions and attitudes towards IT risk and information and its protection. Conversely it was stressed by some participants that in their experience individuals displayed increased propensity for risk-taking if they observed their colleagues doing the same. A number of means for visibly demonstrating and embedding risk culture were noted including demonstrating desired value and behaviour patterns towards IT risks and information security, management strategies and security awareness campaigns and measures as significant mechanisms to embed a risk aware culture. Mentoring and the use of experts to convey risk messages were further noted as significant mechanisms for establishing risk values and norms.

The majority of participants noted the influence of subjective perceptions on risk awareness. One participant remarked: *"There is an indication that individual level factors can impact on risk awareness and there is a requirement to ensure individual biases are identified and addressed".* A number of perceptual biases were identified in the experience of the participants including unfounded optimism among individuals that risks will not occur to them. Several respondents commented that this perception frequently led individuals to significantly underestimate IT risks. Another identified bias related to the perception of control in which it was noted that the more employees felt in control of their immediate IT activities the lower the perception of risk. Participants also underlined that individuals tended to under-estimate risks as a result of their liking or enjoyment of certain activities, such as engagement in social media. A number of participants shared the view that robust compliance and governance processes through reinforcing awareness of the risks and the sanctions which may follow could be a strong potential mechanism for countering the effects of these biases. Another participant highlighted the role of emotions in risk awareness:

"Risk awareness of compliance issues is one area where there is always anxiety because of the fast changing environment. Peoples' attitudes can affect the perception of the risk because if there is fear or lack of understanding then there is less commitment to developing awareness."

The consensus emphasised a moderate level of employee awareness of IT risk beyond their own context to the whole organisation and different departments. Prompting employees to enlarge and widen their risk perspective was noted by some participants as significant for improving risk awareness as employees may potentially become more cautious and risk aware when they are conscious of the impacts of risks on other people and departments. One respondent stated that: *"There is definitely more scope to ensure that employees have a broader understanding of the other departments work contexts and the nature of roles in different areas."* Another respondent emphasised:
Employees need to acquire and understanding of IT risks not only in context of individual or team processes but in terms of safeguarding wider interests.

There were views that responsibility for risk awareness can be placed on individual employees and teams: "*We have to allow employees the opportunity and freedom to explore and generate free flowing communications…actually people become aware not through a process of completing check but learning in the job…so we have to build this into the culture."* The suggestion is that if it is free flowing then new risks can be identified and the organisation is not regimented in ticking off existing already identified risks.

The consensus among the participants emphasised that sole reliance on gathering information on risks was insufficient to enhance risk awareness at an organisational level. Combinations of factors were identified by participants including assessment of susceptibility and vulnerability to risk and the management of knowledge. The participants emphasised challenges in managing this issue in isolation and advocated a more integrated and cross-departmental approach in addition to the need for a more formalised implementation of risk awareness.

The majority of respondents also demonstrated the view that risk awareness involved apprehension and understanding of risks which may not necessarily have visible impacts. This was emphasised to be particularly applicable in the IT context as many threats, unless

detected by computerised security measures, would remain hidden from individual perception. It was felt that this area was generally an organisational strength as many less visible threats were perceived as highly critical therefore awareness was important.

5.4.4 Conclusion

The findings emphasise the utility of the MERIT model for conceptualising risk awareness and emphasise that it is a complex phenomena consisting of and influenced by a range of different subjective elements including cognitive, social, cultural, psychological, attitudinal, emotional and behavioural components which need to be considered and addressed within risk awareness implementations. In addition risk awareness is critically dependent on knowledge flows and the extent to which people understand a range of different types of risk including critical and novel security risks as well as those which are familiar and common.

Chapter 6 Delphi Methods

6.1 Introduction

The IT systems risk awareness conceptual model is composed of six parameters that are significant contributors to enterprise risk management. In this research they are labelled as the risk management processes. Tarantino (2008) lists three elements as Governance, Compliance, and Risk Management in no specific order. Pohlman (2008) further lists five elements as Governance, Compliance, and Risk Management**,** Enterprise and IT GRC in no specific order. These six elements form the MERIT IT Systems Risk Awareness pyramid model and are related and linked to achieve Risk Awareness. This model of the pyramid is an original contribution to risk management knowledge and is the basis to develop a novel conceptual model of IT systems risk awareness.

MERIT IT Systems Risk Awareness pyramid model provides a framework for the development of metrics for measuring people's awareness of risk to IT systems. The model was developed to obtain sound understanding of enterprise risk management and the essential variables that need to measured.

Most research on risk management examines the qualitative aspects of risk management while existing quantitative research seeks to explain risk management rather than provide practical measures of risk management. The MERIT IT risk awareness model expands the knowledge on risk management in terms of understanding the significance of the five elements for measuring risk awareness. The proposed model supports changing the physical system by measuring peoples' awareness of risk in terms of the whole of risk management – governance, enterprise, IT GRC, risk management and risk awareness. Developing IT systems risk awareness metrics would enable risk managers to take appropriate steps to increase levels of risk awareness, thereby improving the effectiveness of enterprise risk management. The Delphi Panel data as applied to the MERIT IT risk awareness model provides empirical data about risk, in this case through a general view of several organisations. But the significance of this method is that it can provide empirical causal data for a specific organisation. The MERIT IT risk awareness model provides data that can be used to control and predict the risk phenomenon.

General application of the outcomes of this research is also possible. Risk awareness metrics improve our understanding of IT risk and can be used to create enterprise-wide risk awareness as part of an IT risk management strategy. Since the focus of this research is on IT risk awareness, the model can be used to develop metrics to assess and develop a prudent risk culture of data and information. Specifically, the risk awareness metrics give employees a stake in IT risk management. This research has academic and economic impact as it could enhance the risk awareness construct. Through better construct definition risk awareness can be more effectively related to risk management strategy. The impact of the research will be direct on existing academic researchers who will be able to draw on the final published dissertation and resulting conference papers. Researchers will benefit from a conceptual construct definition of risk awareness.

6.2 Data Collection Methods

Data to validate the MERIT IT systems risk awareness conceptual models was collected and analysed using a mixed methods approach. Data was collected on managers' and employees' current practices on risk management in multiple organisations in different sectors of the economy. The specific data collected concerned existing practices, levels of risk awareness and professional awareness of risk amongst IT staff. Data was also collected on the specific variables of the MERIT IT systems risk awareness model in relation to these aspects.

The data collection process was divided into three phases. Data on the six elements of the MERITS IT systems risk awareness conceptual model was collected using mixed data collection methods. The data collection process comprised scoping the presence of these six elements in the UAE enterprises, phase one of the research methodology, using ten enterprises ranging from small, medium to large enterprises. These enterprises were asked to respond to 119 questions covering the above six risk management elements and comprising descriptive and analytical statistical data. This data was then used to develop the conceptual model of IT systems risk awareness and management, phase two of the research methodology. This conceptual model was then confirmed in the UAE police force phase three of the research methodology.

6.2.1 IT Risk Awareness and Enterprise Risk Management

IT systems risk awareness is an observable variable of IT systems risk management. It is modelled as a function with five independent variables. IT risk awareness is a mechanism intended to facilitate rapid response to manifestation of negative incidents relying upon the practical knowledge and shrewdness of all staff members.

Thus, risk awareness (RA) is a function of compliance (C), governance (G), enterprise (E), IT GRC and risk management process (RM). It can be expressed mathematically as:

$$RA = f(G, C, E, IT\ GRC, RM)$$

All the G, C, E, IT GRC and RM variables have values ranging between 0 to 100%.

The core RA function is a variable in the overall MERIT Risk (MR) function. The MR function determines the level of enterprise risk management through measurement of risk awareness (RA). Thus, measurement of MR through RA reflects the other five independent functions which are fundamental parameters of RA. They collectively form risk management activities of an entire organisation. This is shown in Figure 13.

MERIT Risk = MR

$$MR = f(\text{Risk Awareness}) = f(f(G, C, E, IT\ GRC, RM)) \text{ ---------- (Equation 1)}$$

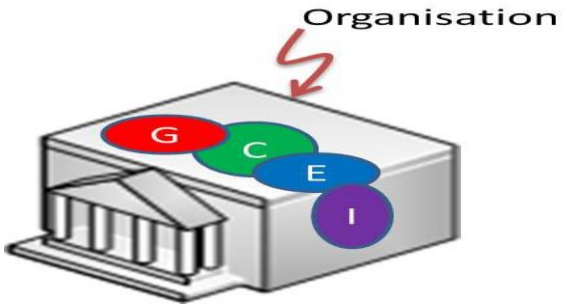

Figure 13 G, C, E and IT GRC forms an entire organisation

In the real world, some of these risk management activities may be overlapped. However, there is very little impact on the entirety of the organisation if it is assumed that G, C, E and IT GRC are not overlapped as depicted in Figure 14.

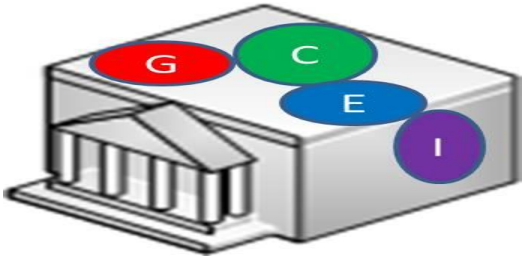

Figure 14 G, C, E and IT GRC not overlapping

Risk management is based on G, C, E & I activities within the organisation. Therefore, evaluating the risk by considering the RM function is extracted from known risk management activities. Risk Awareness (RA) on the other hand, is observable as the risk behaviour of staff which means attitude, skills and experiences of staff in Risk Management and Risk Awareness. Some staff, depending on their role, may have excellent experience of determining risk or risk-averse behaviour, but new staff may require training and special skills to arrive at the same skill levels as the experienced staff. Therefore, risk awareness is another parameter which can be considered dependent on RM. RM and RA are shown in Figure 15 as input parameters to the entire organisation.

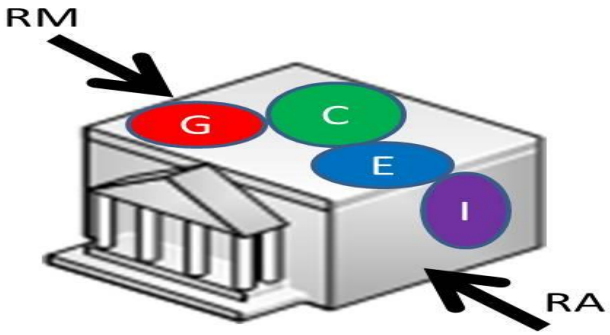

Figure 15 RM and RA are determining the risk of the entire organisation

RM and RA help to protect the organisation from failure or becoming undervalued. So, if RM is estimated as zero, MR is zero. The same applies to RA; MR is zero if RA is zero. Hence, MR could be expressed as the following equation and depicted in Figure 16. Hence, it is evident from Figure 16 and equations 1 and 2 that effectiveness of enterprise risk management is based on the overall risk awareness and risk management.

MR = f (RA) = RM * (I + E + C + G) ---------- (Equation 2)

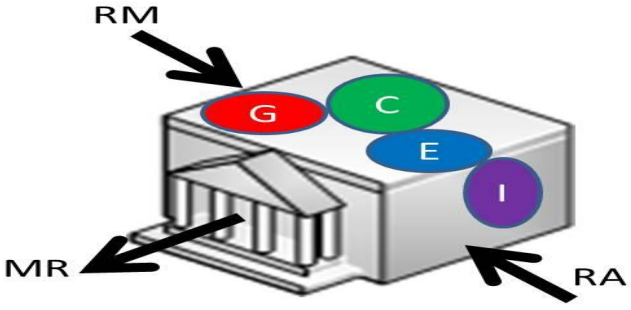

Figure 16 RM and RA can maximise MR for entire organisation

Where: I = ITGRC, E = Enterprise, C = Competence, G = Governance. These elements of the model are added because they have a compound effect on risk management.

6.2.2 Governance Model

Governance is the system by which the organisation is directed and controlled. It can be applied at international, national, local, and organisational levels and to manage organisational resources. There are numerous governance models but this research focuses on a system that is suitable for the police force in the UAE and would have general application for government enterprises.

The performance of governance (G)

All organisations have a framework, directions and rules that achieve the targets and objectives of the organisation which is understood under the term of governance. Decision making at all hierarchy levels, strategy formulation and implementation to achieve the mission and goals of the organisation are influenced by governance mechanisms in place. Employees are required to understand and adhere to governance directions rapidly and, if the governance is well communicated, provide positive feedback. Such feedback enables the role of governance to enhance responsibility within decision making to improve the organisation. The governance mechanism can influence operational efficiency and quality of services. Further utilisation of effective elements of governance such as policy, planning, process, managing and identifying external and internal risks that affect the business will reduce the overall risk for organisation. Therefore, good governance allows employees to increase their risk awareness. Therefore governance should encourage an information risk awareness culture within an organisation with positive feedback in the time permitted.

The risk governance function (G) is dependent on three variables: the guidance (g) on risk provided by the enterprise, employee feedback (f) on the guidance provided and the extra time (T) that the employee would take to understand and react to guidance provided. Changes in g, f and T would affect G. Hence, governance (G) can be expressed as

$$\textbf{Governance (G)} = f\textbf{(g, f, T)}$$

Value of G is to be obtained in terms of % from 0 to 100%.

Where:

g = The risk directions or guidance of the enterprise that any enterprise would follow. Any changes in these directions will change G. In other words, employees need to know and

understand these directions. The more the employees understand and follow the directions the higher value of g, the more G improves and vice versa. Therefore, g plays an important role to change G. **g can take any value between 0 to 100%, any increase in g will increase G.**

f = But g is linked with the positive or negative feedback (f) of the employees. The feedback will provide a degree of controllability or knowledge to the directions of the enterprise. If employees understand the directions of their enterprise, then they will give positive feedback, which will increase G. If all required guidance has been applied then there is no feedback, G will gain highest positive percentage value. On the other hand, if the feedback is maximum; that is the guidance has not been implemented or wrong guidance issued, G will be zero percentage. **f can take any value between 0 to 100% and any increase in f will increase G.**

T = The third variable that plays an important role and changes G is time (T). This time specifies the number of days that employees require to become familiar/understand and apply the issued guidance. Employees do need time to understand the directions of the enterprise. The quicker the employee learns the guidance, the better the value of G. This means that, where each employee understands and knows the directions of the enterprise they will offer no feedback (positive feedback) and hence enhance the G value. The shorter time to understand will lead to a higher G value and a longer time will lead to a lower G value. The minimum trial in the case company is 90 days for each employee to become familiar and understand the directions of the enterprise.

T = Time to understand and apply issued directions (365 days)
Max Trail = (T – trail) Min = 365 – 90 = 275 days.
T can take any value between 0 to any number of years required as extra time: for example a 1.5 year increase in extra time required will decrease G

$$G = \frac{g \times f}{100} \times \frac{365 - T}{275}$$

This function can be plotted as follows:

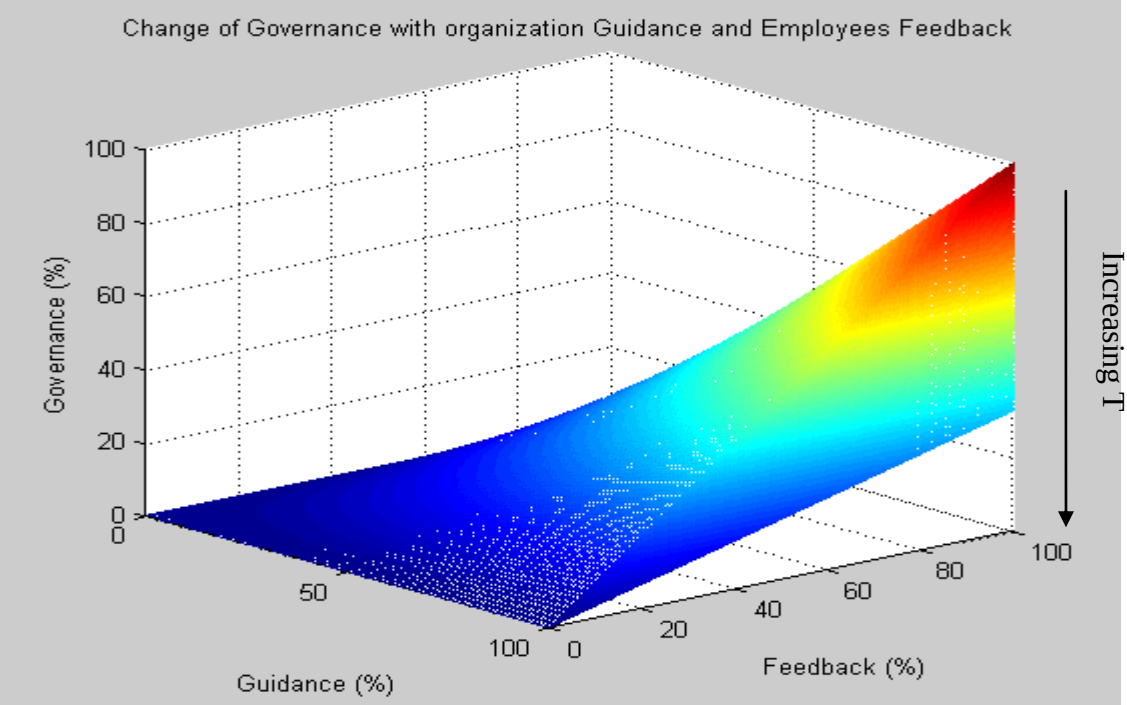

Figure 17 Governance Function Graph

It can be noted from Figure 17 that when the feedback and guidance are effective (f=100% and g=100%), for a minimum familiarisation time of 90 days the governance is at its maximum (G=100%). If either the feedback or the guidance is null, the governance is null.

Table 7 summarises the scenarios generated above for the G function in terms of g and f. Both variables g and f can affect along with time. For ease of understanding, the T value has been kept constant at 90 days and 275 days.

The findings show increases in feedback of employees' time indicating that the quality of governance is low. The G function metric can be used to gauge the quality of risk governance and take appropriate action when it is low. The result potentially underlines weak governance, poor risk communication, or employee induction and training methods for risk management need improving.

Table 7 Governance scenarios

f	G	G Where T=90 days	G Where T=275 days
10	10	0.96	0.29
20	20	3.87	1.18
30	30	8.71	2.65
40	40	15.47	4.71
50	50	24.18	7.63
60	60	34.82	10.61
70	70	47.39	14.43
80	80	61.91	18.85
90	90	78.34	23.85
100	100	96.73	29.45

The above table shows that when employees take a longer time than the permitted trial time to become familiar with the governance, G becomes inefficient to 29.45%. Otherwise, the function G performs well, given positive feedback and a short trial time of 90 days. In conclusion, f, g and T play an important role for G. This implies that when any organisation directs and controls their employees this will make the feedback positive, which increases their knowledge, skills, experience and performance within the allowed period.

6.2.3 Compliance Model

Effective organisational compliance mandates that employees need to observe the requirements of government regulations and adhere to the policies to comply with the regulations in order to reduce any risk. Therefore, the organisation must set up policies and procedures to comply with regulations by increasing the level of knowledge and skills of employees in accordance with the requirements for compliance. Regulations require that data should be stored securely. Governments make laws to prevent misuse or loss of public information or data. The organisation has to make sure that employees are familiar with these regulations and how to comply with them. Organisations must make sure any stored data is

stored securely. To support risk managers decision-making on compliance the following mathematical function has been created.

Thus, compliance (C) varies with employee understanding of applications (App.), time taken to gain knowledge of regulations (T) and feedback of employees (f).
Thus, compliance C can be expressed as:

$$\mathbf{C = \mathit{f}\ (App., T, f)}$$

Wherein, **Value of C** in terms of % that is 0 to 100%

App = Employees understanding of the compliance requirements and how they apply them in practice, and the way they deal with customers, range of values from 0 to 100%.

Tkn = Knowledge of regulations gained via workshop or training on compliance and how long employees have been with the organisation. Range of values for 0 to 275 days, the shorter time that employees take to understand the better the compliance.

f = Feedback to employees from internal managers or external feedback from governance authorities and customers. Range of values for feedback would be 0 to 100%. Positive feedback indicates good or higher level of compliance.

The compliance, on the other hand, is a function of the applications of the organisation App (%), the feedback received from the employees f (0% means positive feedback, 100% negative feedback), and the time taken to understand these applications, Tkn (days). Since the minimum time is set to 90 days and a maximum of 275 days, the formula for the compliance takes the form:

$$C = \frac{App \times f}{100} \times \frac{275 - tkn}{275}$$

This function C can be plotted as shown below in Figure 18.

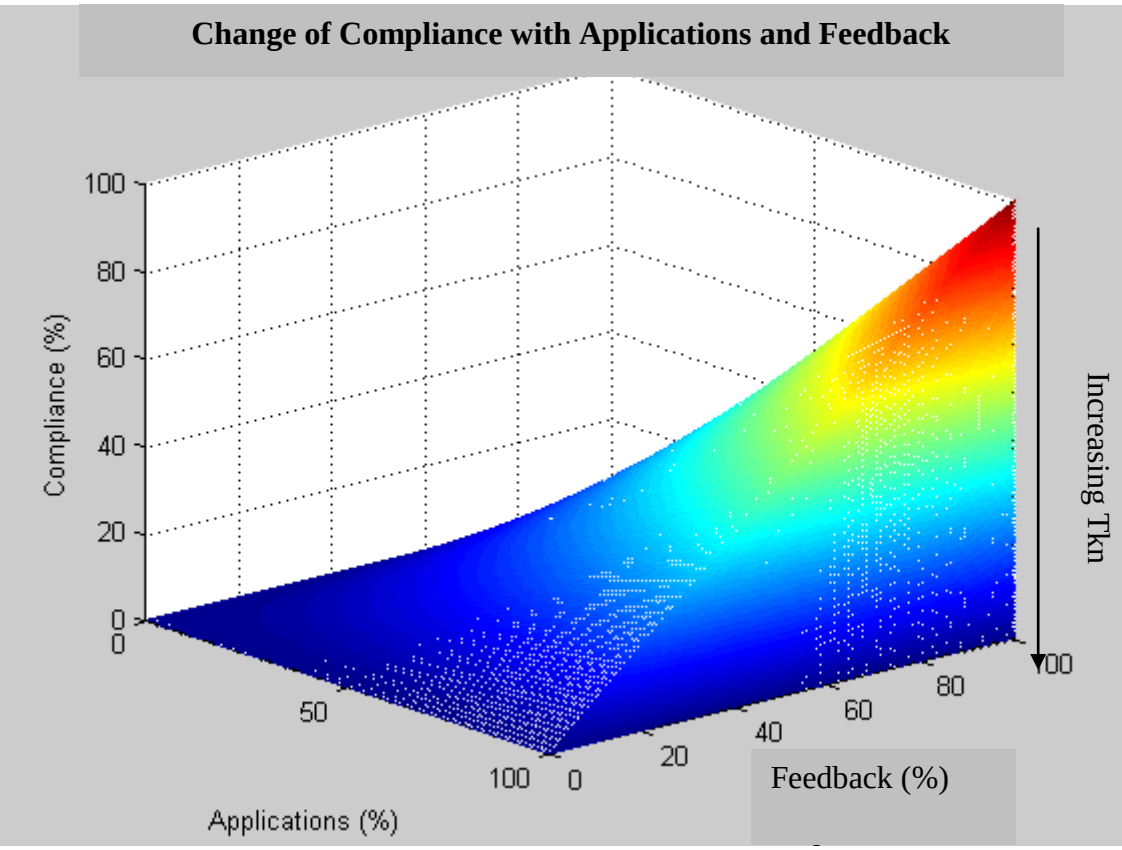

Figure 18 Compliance Function Graph

Table 8 summarises the scenario analysis value of C in terms of the variables f and app. where employees have taken time either 90 days or 274 days. Compliance is considered ineffective when time taken is 274 days irrespective of feedback and knowledge. Compliance is an activity which requires all level of hierarchies to be alert and proactive.

Table 8 Compliance scenarios

App. %	f %	C % Where tkn=90 days	C % Where tkn=274 days
10	10	0.68	0.004
20	20	2.69	0.015
30	30	6.05	0.032
40	40	10.76	0.058
50	50	16.81	0.090

60	60	24.21	0.131
70	70	32.96	0.172
80	80	43.05	0.232
90	90	54.49	0.295
100	100	67.27	0.366

In conclusion, f and app. play an important role for C within permitted limits of Tkn. As one can see from the above table that even if understanding and feedback based on the understanding and training for risk awareness and management is 100%, how many days an organisation takes to achieve such results count for overall risk awareness. Thus, compliance can be considered 100% when employees understand the risk awareness and management in the shortest possible time or far less time as compared to industry standards. Therefore, good compliance in any organisation should encourage employees to follow the compliance requirements to improve their knowledge, therefore resulting in positive feedback which will help towards the required level of compliance.

6.2.4 Enterprise Model

Enterprise is a project or a mission that produces products and services. The enterprise E is a function of the size of the organization s (0 to 100%, where 100% is large), the quality of the products (%) and the feedback from the customers F (%)

$$E = \frac{Qu \acute{} F \acute{} s}{10^4}$$

Where

Qu = Quality of products and services that the organisation provides. The range of values is form 0 to 100 where 0 is poor quality and 100 optimum quality.

F = Feedback on products and services from the customers and governance. The range of values is from 0 to 100 where 0 is positive feedback and 100 is negative feedback.

S = Size of enterprise large, medium and small. The size of enterprise gives a good indication to the organisation performance because there will be more employees that produced a good services and products. Also they will be more aware of risk. The range from 0 to 100 and large = 100.

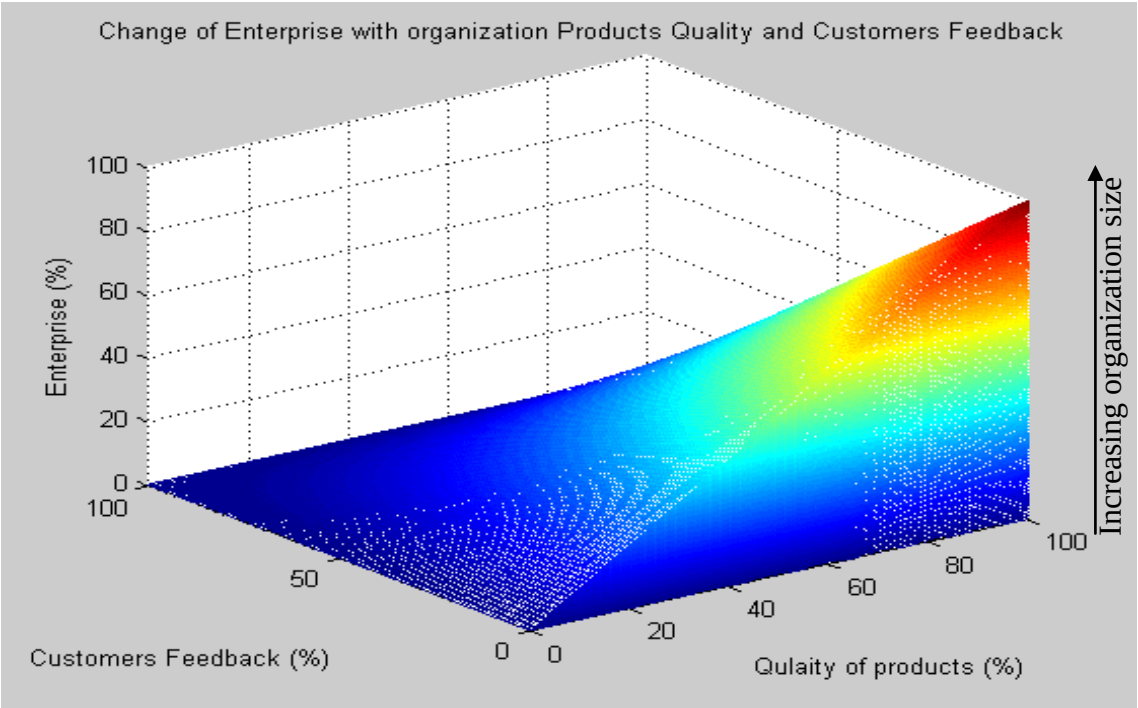

Figure 19 Enterprise Function Graph

It is assumed here that large organisations can implement and benefit from governance, compliance, risk management as the human capital advantage for them is the highest. Stemming from the resource based view of the organisation, human capital advantage is important. However, there is a trade-off between costs in governance, compliance and training implementation due to the changing demographic of employees.

Table 9 Enterprise scenarios

Qu %	**F %**	**E (%) Where s=50%**	**E (%) Where s=100%**
10	10	0.5	1.0
20	20	2.0	4.0
30	30	4.5	9.0
40	40	8.0	16.0
50	50	12.5	25.0
60	60	18.0	36.0
70	70	24.5	49.0
80	80	32.0	64.0

90	90	40.5	81.0
100	100	50.0	100.0

6.2.5 IT GRC Model

Making use of IT GRC, I (%) is a function of three variables: u: the unification, int: interconnections and sk (%) the total IT technology skills:

$$I = \frac{1}{12} \times me \times \frac{1}{n} \times sk$$

Where, ***me*** is the number of meetings and ***n*** the number of employees.

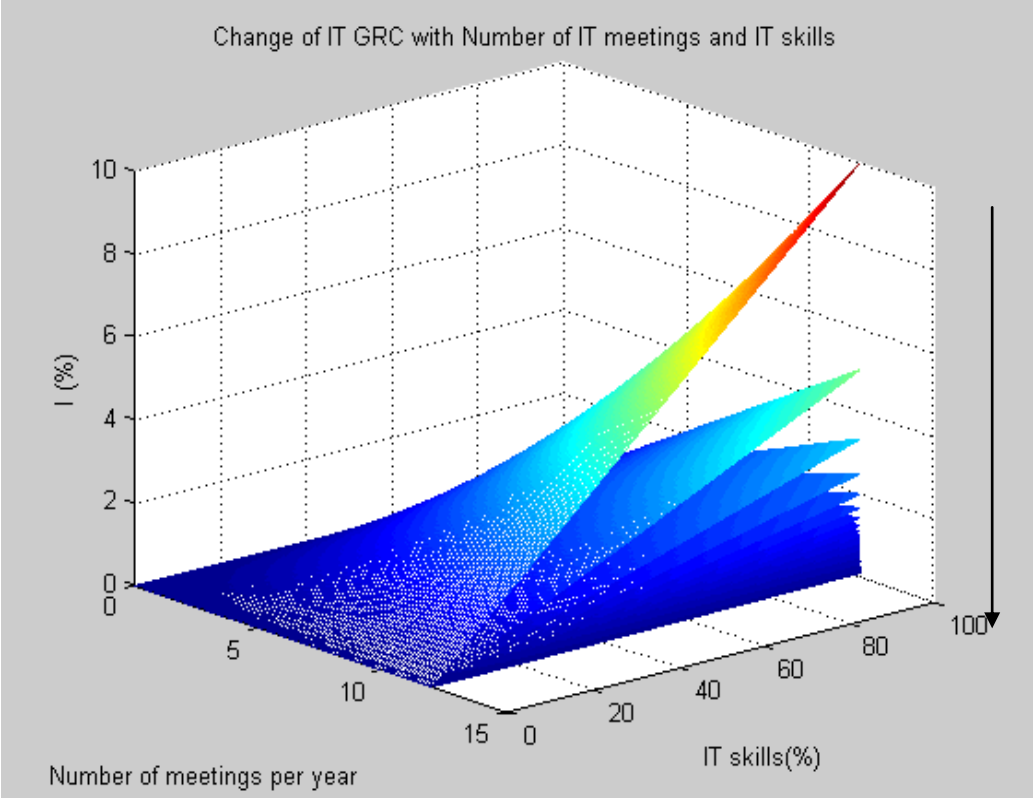

Figure 20 IT GRC Function Graph

The lattices in the graph depict the frequency of the meetings, where large organisations have more meetings to communicate and the smaller ones have less. This function largely depends on the skills achieved in reality rather than how many employees meet how many times. It is evident that if an organisation has 1000 employees as compared to 100 then these employees would need more meetings and training sessions. The main assumption is that with each

meeting or increase in employees, the skills level or human capital for an organisation would increase.

Table 10 IT GRC scenarios

me %	sk %	I (%) Where n=1000	I (%) Where n=10
10	10	O.00	0.83
20	20	003	3.33
30	30	0.075	7.50
40	40	0.133	13.33
50	50	0.208	20.83
60	60	0.30	30.0
70	70	0.408	40.83
80	80	0.533	53.33
90	90	0.675	67.50
100	100	0.833	83.33

6.2.6 Risk Management Process Model

The risk management is related to risk management process rmp (%), the performance P (%) and the time taken to manage the risk Tr (days) (maximum time is 90 days).

rmp, in turn, represents the average of the risk identification Ri, risk assessment Ra, and risk control Rc. That is rmp = (Ri+Ra+Rc)/3.

Consequently, risk management is expressed as:

$$RM = \frac{Ri + Ra + Rc}{3} \times \frac{(90 - Tr)}{90} \times \frac{P}{100}$$

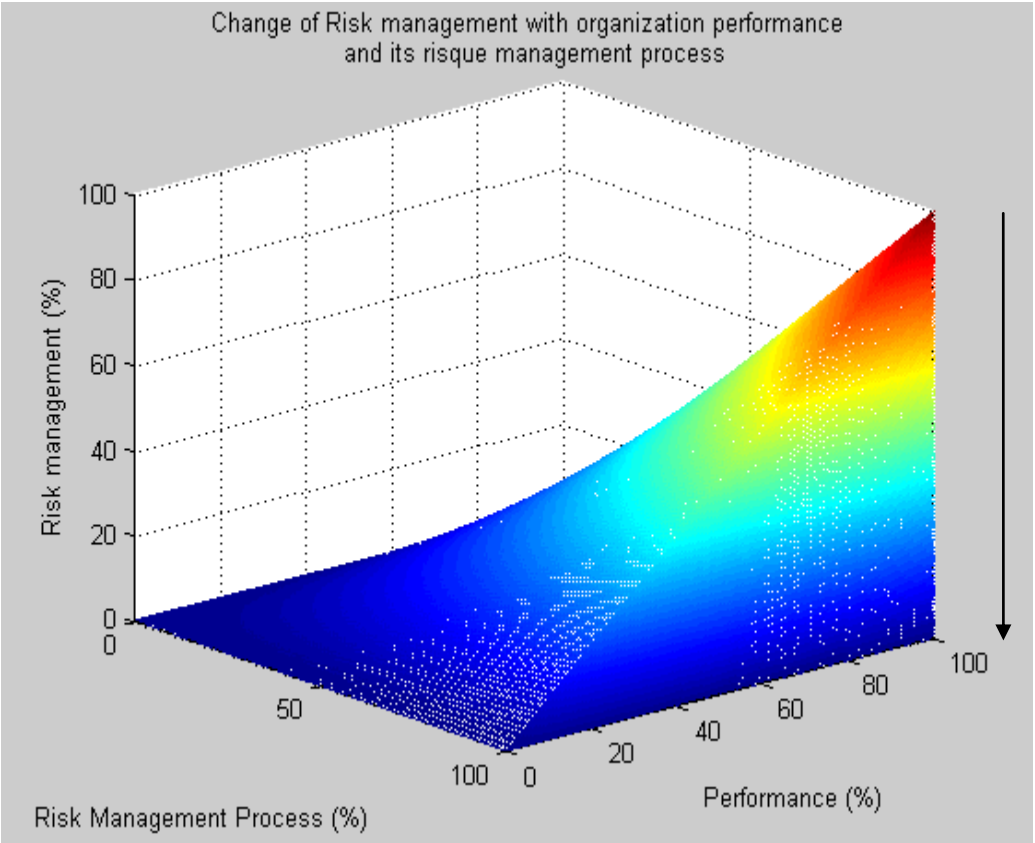

Figure 21 Risk Management Function Graph

Table 11 Risk management process scenarios

rmp %	P %	RM (%) Where Tr=45 days	RM (%) Where T=85 days
10	10	0.5	0.05
20	20	2.0	0.22
30	30	4.5	0.50
40	40	8.0	0.88
50	50	12.5	1.39
60	60	18.0	2.00
70	70	24.5	2.72
80	80	32.0	3.56
90	90	40.5	4.50
100	100	50.0	5.56

Table 12 Risk Awareness scenarios

rmp %	Tr days	RM (%) Where P=100%	RM (%) Where P=50%
10	10	8.89	4.44
20	20	15.56	7.78
30	30	20.00	10.00
40	40	22.22	11.11
50	50	22.22	11.11
60	60	20.00	10.00
70	70	15.56	7.78
80	80	8.89	4.44
90	90	0.0	0.0
100	100	-11.11	-5.56

Substituting equations all formulae for G, C, E, IT GC and RM in equation (2) for RA gives:

$$RA = \frac{Ri + Ra + Rc}{3} \times \frac{(90 - Tr)}{90} \times \frac{P}{100} \times \left(\frac{me \times sk}{12n} + \frac{Qu \times F \times s}{10^4} + \frac{f \times (g \times (365 - T) + App \times (275 - Tkn))}{2.75 \times 10^4} \right)$$

The function of RA against performance P and quality of products Q can be plotted as below whilst rest of the variables in the above main RA equation are constants.

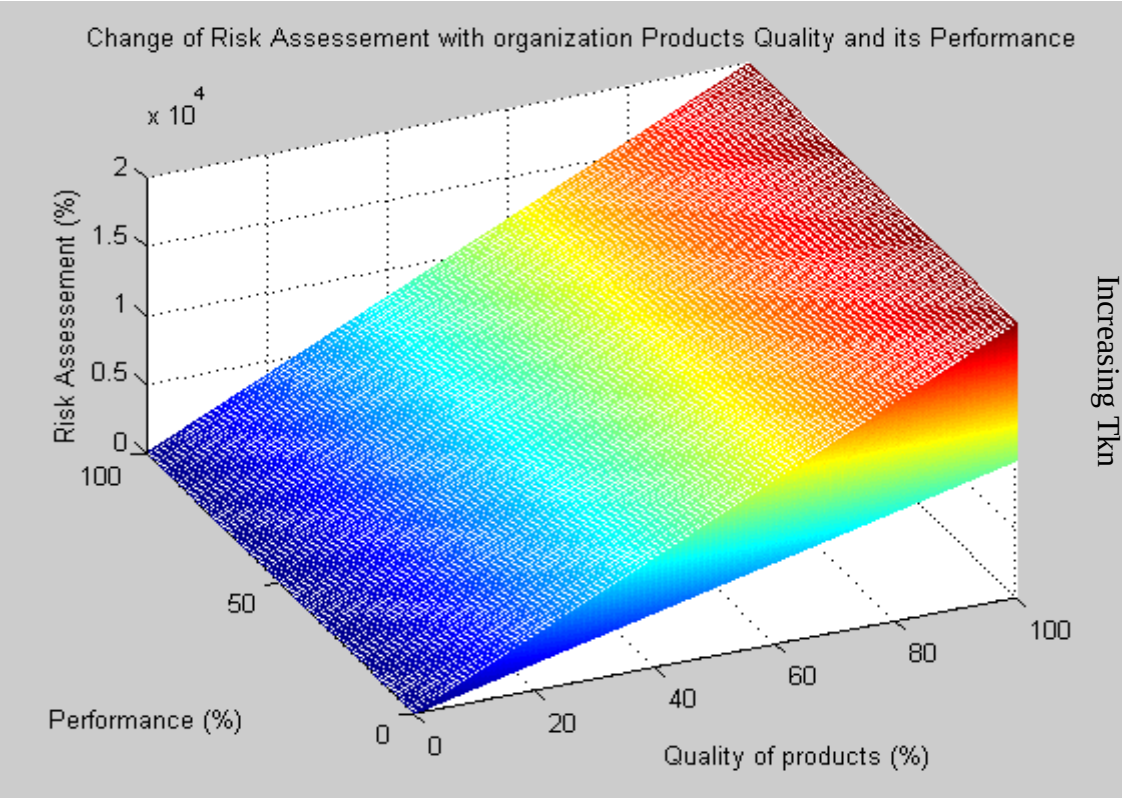

Figure 22 Risk Awareness Function Graph

6.3 Enterprise Learning

The success of IT systems depends on how well the enterprise learns to adopt technology and how well members of the enterprise adapt their behaviour to accept new technology. An aspect of this acceptance concerns enterprise learning of risk behaviour. Rau and Haerem (2010) studied 'exploration' and 'exploitation' behaviours of people who control new technology or 'gatekeepers'. "Exploration includes things like search, experimentation, risk taking, discovery, and innovation, while exploitation includes things like refinement, efficiency, implementation, and execution" (March 1991).

It is proposed here that improved levels of IT systems risk awareness can result from valid conceptual models that lead to empirically measurable variables affecting IT systems risk awareness. It is important to appreciate that IT risk awareness metrics need to be absorbed into the enterprise through enterprise learning.

Over-reacting to risk by placing constraining and burdensome controls on people can reduce normal initiatives and productivity in enterprises. Therefore, a considered use of risk controls is necessary. Young's (2010) study found that "enterprises that exhibit higher levels of

collaborative exchange and develop and implement more information security policies are more effectively utilising the information security strategies of detection, deterrence and recovery" (p.19).

6.4 Delphi Method

6.4.1 Delphi Method Analysis

The Delphi method was used to confirm empirically the MERIT IT Risk Awareness conceptual model. Empirical data on the variables of the model were collected from expert departmental managers and IT managers in the rounds of the Delphi method. This was done to validate empirically the variables stemming from the MERIT IT Systems Risk Awareness conceptual model obtained from the review of the risk management and IT risk management literature.

This empirical validation strengthened the model's application to evaluate IT systems risk awareness in organisations. The Delphi method was selected for two reasons. One, it would collect experts' knowledge on IT risk awareness. Two, it could be applied for policy-making based on the consensus of experts.

The selection criteria for the experts were derived from experiential knowledge of IT risk management and from reading the literature on risk management and IT risk management. These criteria included (a) five years' experience in a managerial role, (b) significant risk management responsibility and (c) demonstrated success in risk management, as noted in their curriculum vitae. The experts consulted were IT security engineers, CCTV experts and IT engineers.

The panel of experts independently and separately answered questionnaires in two or more rounds and in each round they should revise their answers based on an independent expert's summary of their answers. The independent expert, the facilitator, is used to provide an anonymous summary of the experts' forecast from the previous round and gives the reasons for their judgements. The aim is to decrease the range of answers during this process towards a standard or correct answer. The process is stopped when the predefined stop criterion is reached, usually number of rounds or achievement of consensus. The mean or median scores of the final rounds constitute the results. The method is illustrated in Figure 23.

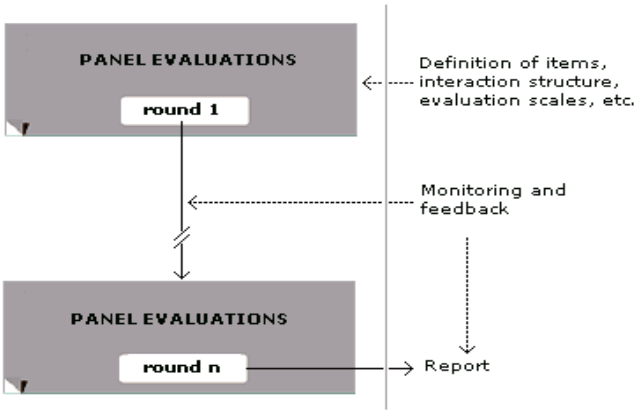

Figure 23 The Delphi Method communication structure

(Source: Okoli and Pawlowski, 2004)

The Delphi method has the following features: panel of experts, facilitator, structured information flow, regular feedback and anonymity of participants (Okoli and Pawlowski, 2004). These features help the participants to focus on the issue explored and provide expert knowledge on the topic under investigation. A panel of experts in the field is chosen and the questionnaire is given to them and the answers collected. There is no stipulation for the size of the panel of experts. In large panels, a panel director manages the interactions among participants by editing the information and filtering out irrelevant content. This helps to structure the information flow. The regular feedback is composed of participants´ own comments on their forecasts, the responses of others and the progress of the panel.

All the panel experts remain anonymous and their identity is not revealed, even when the final report is completed. This curtails social pressure to conform, for example the authority, personality or reputation of other experts may dominate. Anonymity prevents experts from taking defensive postures to defend their original answers. Social pressure is not used to sway experts to the majority or consensus view. This is done by enabling experts to see others' answers and then revising their own answers. Anonymity thus facilitates free expression of opinions, open critique and admission of errors when revising earlier round answers. It is argued that anonymity also frees experts from their personal biases and minimises the 'bandwagon effect' or 'halo effect'. The role of the facilitator is crucial in the Delphi method. The facilitator manages the Delphi rounds and ensures that the participants follow instructions. The response are collected and analysed and common and conflicting answers are identified. The facilitator seeks consensus and if it is not reached the process continues until the answers synthesise towards consensus.

Delphi method uses scales to obtain answers. This research used scales. Examples are shown and the complete Delphi questionnaire is given in Appendix E. The Delphi method was used as the following five steps described.

Define the problem

Identify the problem that needs to be resolved. This was done by reading the literature on risk management and IT risk management, formulating the conceptual model and the mathematical model. The variables of the mathematical model required empirical validation to validate the mathematical model. These variables from the 5 mathematical functions of the model were then posed as quantitative questions in a questionnaire on IT risk awareness to the Delphi experts.

Distribute the questionnaire

Identify the Delphi experts capable of addressing the problem. Once the problem is defined it needs to be distributed to the experts. The Delphi group experts were chosen from the researcher's experiential knowledge and contacts in private and public organisations. The researcher has over 20 years' experience working in the police force and an active network of experienced managers in private and public organisations. Some of these expert managers and IT managers were recruited to join the Delphi group. The Delphi method does not require meetings, since experts answer the questionnaire individually in separate rounds. The number of Delphi experts chosen was 6, which is considered to be adequate. The questionnaire or problem was sent to the Delphi experts and they were asked to respond. The administration of the questionnaire was done by the researcher, ensuring that Delphi experts had received the questionnaire and prompting them to respond where necessary and that the feedback from the independent expert was communicated to the Delphi experts.

Collate the responses

The researcher collated all the responses into one list. The annotations to the questionnaire in the different rounds were made simple for Delphi and independent experts to read and the annotations were communicated to them verbally to avoid misunderstanding. Since, scale scores were being collated the likelihood of bias was minimal.

Give everyone the collation

The researcher sent the collated answers to the Delphi experts. They were asked to score each item on the given scales in the questionnaire. The Delphi method permits addition of further items as appropriate but no new items were needed.

Repeat as necessary

The Delphi method places no minima or maxima limit on the number of iterations of the process. The aim is to achieve consensus of answers from the Delphi experts. Two rounds were judged to be sufficient because the scores tended towards consensus levels.

6.5 Data Analysis Methods

Data collection needs to consider two aspects: what data to collect and how to analyse it. The former was covered in Section 6.2 above. How the data was analysed in detailed in this Section.

6.5.1 Measures of centralisation, dispersion and cluster analysis

The statistical data were ranked in order of magnitude to obtain the mean. The mean is a statistical model of the data. It is the hypothetical value of the data which enables conceptualising risk management. It was obtained by using the following formula:

$$\bar{X} = \frac{\sum_{i=1}^{n} Xi}{n}$$

The mean is the measure of central tendency of the data but not actually observed in the phenomenon. Where X bar is the mean, Sigma the sum of individual observations and, *n*, the number of observations. It was used to summarise the survey data. The mean provided the average score which helped to determine the central tendency of the data and this enabled conceptualising risk management in the UAE enterprises.

The mean statistical model was then assessed to see its fit. The standard deviation was used to see how closely the mean resembles the real practice of risk management. The standard deviation is the square root of the variance of the data from the mean, where sigma is the sum of the individual observations minus the mean. It is obtained by using the following formula:

$$s\sqrt{\frac{1}{n-1}\sum_{i=1}^{N}(Xi-\bar{X})^2}$$

The survey data was analysed to determine clusters. Cluster analysis was used because it enabled the discovery of significant similarities or groupings among the data. In cluster analysis, classifications are determined empirically, statistical analysis of the empirical cases. This was important to understand patterns in the data that signify important risk management concepts and thereby understand actual risk management practice. This information was then used to support the construction of the model.

6.5.2 Descriptive and categorical qualities

The purpose of qualitative data analysis is to understand the meanings of peoples' actions (Patton, 1987). The interview data was analysed by developing categories. Categorisation is a standard technique in qualitative data analysis (Romesburg, 1984). It involves examining the data to find recurring meanings that form patterns. The qualitative data was analysed to discover significant patterns of meanings relating to risk management.

6.5.3 Expert Knowledge Delphi Method

The conceptual model was validated using the Delphi method. The questionnaire comprised questions on the variables composing each of the six factors, Governance (four questions), Compliance Model (four questions), Enterprise Model (three questions), IT GRC Model (three questions), and Risk Management Model (five questions) in total, nineteen (19) questions. Since the variables of the variables were interval values, a scale measure was used with percentage units, actual days, or absolute values depending on the variable. In one question, categorical data was collected for firm size, small, medium or large and allocated the equivalent percentage values 33 per cent, 66 per cent and 100 per cent to enable calculation.

The data of the Delphi method are analysed as part-and-partial of the data collection process. As noted above in Section 4.4.3, the Delphi questions are administered to experts and collated in successive rounds, to obtain a consensus view among the experts.

To analyse the scores, the method used in Delphi analysis for smaller groups was used. This method is suggested when percentage scores are used. This method is the formula:

$$v = (s_l + s_h + 4 * Ave)/6$$

This formula emphasises the average more by considering the influence of outlying values. This is especially when percentage scores are used, where S_l is lowest score and S_h is highest score, add 4 and multiply by average score and divide by 6. This gives more weight to the average whilst also allowing some influence from outliers.

For each item in the list of questions, the mean value was calculated and items with a mean greater than or equal to 2.0 were removed. Then the list of questions was returned to the expert panel. They were then asked to consider the reasons for their choices and complete the questions again by considering the mean value.

Al-Shehab (2007) proposed a new model by examining casual and cognitive mapping methods for the identification of risk in IT development projects. The CorMod model proposes a number of desirable characteristics through evaluations based on the Delphi data survey, a questionnaire method involving expert employees in successive rounds to form consensus.

6.6 Delphi consensus values and the IT risk awareness conceptual model

The conceptual model was derived based on literature, logic and scenario analysis in chapter three. However, critical values were obtained through use of Delphi consensus survey wherein final answers were calculated after two rounds of expert panel recommendations for variables included in the risk awareness components: governance, compliance, enterprise, IT GRC and risk management. A summary of the Delphi consensus is shown in Table 13, which shows the analysis of the responses of the Delphi risk management experts' panel.

Table 13 Risk Management Delphi Experts' Panel Response Analysis

C1	C2	C3	C4	C5	C6	C8	C9	C10	C11	C12	C13	C14	C15	C16	C18	C19	C20	C21	C22	C23	C24	
								Ind Expert's									Ind Expert's		Change	Differennce	Consensus	
Governance Model	**First Round**					**St Dev**	**Mean**	**Score**	**Difference**	**Second Round**					**St Dev**	**Mean**	**Score**	**Difference**	**in Mean**	**in Rounds**		**Governance Model**
Question	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5					Expert 1	Expert 2	Expert 3	Expert 4	Expert 5								Question
1	85	25	20	75	75	30.90	56.00	95	-39.00	90	50	83	85	80	15.85	77.60	95	-17.40	21.60	-21.60	76.20	1
2	90	25	5	80	50	35.88	50.00	0	50.00	50	25	0	0	40	22.80	23.00	0	23.00	-27.00	27.00	24.33	2
3	30	90	30	80	30	30.33	52.00	90	-38.00	60	75	80	90	45	17.68	70.00	90	-20.00	18.00	-18.00	70.67	3
4	75	25	40	50	50	18.23	48.00	70	-22.00	75	25	60	65	55	18.84	56.00	70	-14.00	8.00	-8.00	58.00	4
Compliance Model																						**Compliance Model**
5	50	25	10	50	20	18.17	31.00	80	-49.00	80	25	73	75	50	23.01	60.60	80	-19.40	29.60	-29.60	57.20	5
6	90	25	5	75	80	37.58	55.00	0	55.00	50	25	75	0	50	28.50	40.00	0	40.00	-15.00	15.00	31.67	6
7	90	10	25	100	100	43.87	65.00	100	-35.00	100	75	80	100	100	12.45	91.00	100	-9.00	26.00	-26.00	85.33	7
8	50	25	60	45	30	14.40	42.00	80	-38.00	70	50	75	75	50	12.94	64.00	80	-16.00	22.00	-22.00	62.00	8
Enterprise Model																						**Enterprise Model**
9	90	75	80	90	90	7.07	85.00	90	-5.00	90	75	80	95	90	8.22	86.00	90	-4.00	1.00	-1.00	87.00	9
10	95	25	85	75	10	38.01	58.00	0	58.00	50	25	85	75	10	31.90	49.00	0	49.00	-9.00	9.00	35.67	10
11	100	33	66	66	80	24.47	69.00	100	-31.00	100	66	66	66	80	14.93	75.60	100	-24.40	6.60	-6.60	81.53	11
IT GRC Model																						**IT GRC Model**
12	2	3	6	10	6	3.13	5.40	6	-0.60	6	3	6	10	6	2.49	6.20	6	0.20	0.80	-0.80	5.87	12
13	5000	250	8	4000		2558.31	2314.50	6000	-3685.50	6000	250	6000	6000		2875.00	4562.50	6000	-1437.50	2248.00	-2248.00	4292.33	13
14	75	75	90	75	70	7.58	77.00	90	-13.00	80	75	85	85	80	4.18	81.00	90	-9.00	4.00	-4.00	82.67	14
Risk Management Model																						**Risk Management Mode**
15	1	1	1		0	0.50	0.75	1	-0.25	1	1	1		1	0.00	1.00	1	0.00	0.25	-0.25	0.92	15
16	80	25	20	50	30	24.60	41.00	80	-39.00	80	50	78	75	50	15.26	66.60	80	-13.40	25.60	-25.60	62.53	16
17	50	40	20	75	50	19.87	47.00	70	-23.00	60	70	65	75	60	6.52	66.00	70	-4.00	19.00	-19.00	61.00	17
18	75	30	30	50	20	21.91	41.00	70	-29.00	75	30	61	65	30	20.90	52.20	70	-17.80	11.20	-11.20	54.40	18
19	100	50	15	50	30	32.09	49.00	90	-41.00	95	50	80	80	45	21.51	70.00	90	-20.00	21.00	-21.00	69.67	19

Note:

Expert 6's reponses were removed becuase of spoilt response.
Many of the Questions were not answered in the First Round.
All Questions were not answered in the Second Round

Legend

C11 is the difference in the First Round between the Independent Expert and the mean score of the Delphi Experts.
C21 is the difference in the Second Round between the Independent Expert and the mean of the Delphi Experts.
C22 is the change is the mean scores of the Delphi Experts between the two rounds.
C23 is the change in difference betwen the Indepdent Expert and the mean scores of the Delphi Experts between the two rounds.
C24 is the consensus mean among Experts and the Independent Experts, taken as the mean of C8, C9 and C17. This mean is in the same direction as the Independent Expert's score and many variable (Question) are close to the Independent Experts score.

6.6.1 Mean scores and differences of the Delphi panel

The consensus mean, shown in the C24 cell of Table 13, is in the same direction as the Independent Expert's score for each of the variables of the MERIT IT Systems Risk Awareness conceptual model. The values in C24 cell are taken as the consensus values for this model.

The mean score of the risk management Experts in the First Round is shown in C9, the Independent Expert's score in shown in C10 and the standard deviation in C8. The difference between the mean score of the risk management Experts and the Independent Expert is shown in C11. Generally, in the First Round, the scores of the risk management experts were lower than for the Independent Expert for most of the variables (Questions) of the mathematical models. The only close agreement score is the level of feedback variable of the Enterprise Model, showing a small difference of five points between the Experts and the Independent Expert. This general difference is expected and the aim of the Delphi method is to facilitate the formation of a consensus among the experts.

The difference between the experts and the independent expert decreases generally for all the variables (Questions) of the mathematical models is shown in C21 the emerging consensus in the second round when. The experts' mean score of 86 is very close to the Independent Expert's score of 90 for the feedback variable (Question 19).The consensus mean, shown in C24 of Table 13, is in the same direction as the Independent Expert's score for each of the variables of the IT Risk Awareness mathematical model. The values in C24 are taken as the consensus values for substituting in the model.

Governance function is: $G = \frac{g \times f}{100} \times \frac{365 - T}{275}$

Consensus values from the Delhi model are: g = 76.20%, f =24.33% and T = 70.33 days, therefore substituting these values in the above formula G =

Compliance function is: $C = \frac{App \times f}{100} \times \frac{275 - tkn}{275}$

Consensus values from the Delhi model are: App = 57.20%, f =31.67% and tkn = 85.33 days, therefore substituting these values in the above formula C =

Enterprise function is: $E = \frac{Qu \times F \times s}{10^4}$

Consensus values from the Delhi model are: Qu = 87%, F = 35.67% and s = 81.53 days, therefore substituting these values in the above formula E =

IT GRC function is: $I = \frac{1}{12} \times me \times \frac{1}{n} \times sk$

Consensus values from the Delhi model are: me = 5.87, n = 4292.33 and sk = 82.67% days, therefore substituting these values in the above formula IT GRC =

Risk management function is

$$RM = \frac{Ri + Ra + Rc}{3} \times \frac{(90 - Tr)}{90} \times \frac{P}{100}$$

Consensus values from the Delhi model are: Ri = 0.92, Ra =62.53, Rc=61.00, potential of risk occurring = 54.4%, therefore substituting these values in the above formula RM =

6.7 Conclusion

The following Table 14 shows the support for the findings and the proposed conceptual model. The final decision to accept or reject the factor for risk awareness is based on the collective decision of multiple evidences from various types of results. The table includes all primary data analyses.

The data from survey and interview do not directly support the factors. However, the need for training and communication and the existing low level of awareness show that factors such as governance, compliance, enterprise, IT GRC and Risk management are important for overall risk awareness mechanisms and policy implementation.

Table 14 Resulting theoretical framework of risk awareness

Hypothesised Risk Awareness Factors	**Survey in AD police**	**Qualitative Interviews**	**Questionnaire survey of 10 UAE enterprises Dendrograms**	**Histogram analysis**	**K-means analysis**	**Delphi analysis**	**Final acceptance or rejection of factor**
Governance	supported	supported	supported	Supported	Supported	supported	**ACCEPTED**
Compliance	supported	supported	supported	Supported	Supported	supported	**ACCEPTED**
Enterprise	supported	supported	supported	Supported	Supported	supported	**ACCEPTED**
IT GRC	supported	supported	supported	Supported	Supported	supported	**ACCEPTED**
Risk management	supported	supported	supported	Supported	Supported	supported	**ACCEPTED**

It can be seen from the above table that all hypothesised variables or factors are accepted in the final MERIT IT systems risk awareness model. Therefore, there is no change between the initially proposed MERIT IT systems risk awareness model and the one confirmed after analysis of findings.

Chapter 7: Discussion

7.1 Introduction

The purpose of this research is to develop understanding of individual IT risk awareness from an organisational perspective drawing on current and best practice in public and private sector organisations and to propose and validate a holistic model of IT risk awareness which supports understanding through identifying key elements and components of risk awareness. These objectives were achieved through the collection of quantitative and qualitative data utilising three main techniques. A structured quantitative survey instrument and a Delphi panel was employed to validate the six elements of the MERIT model while qualitative data collected through in-depth interviews assisted development of understanding of the different variables identified in literature which potentially underpin risk awareness.

7.2 IT Risk Awareness in the UAE

One of the key objectives of this study was to evaluate the extent, practice and perception of risk awareness in the Abu Dhabi police and in the UAE. The findings show that in the UAE there is a general lack of understanding and failure to maximise the practice of IT risk management in relation to the understanding, usage and level of risk awareness. Risk management still appears to be considered a tick box process except by large organisations such as oil or construction companies which have project management processes embedded in their daily operations. Employees of such companies are more aware of risk than any other organisation. However this is consistent with evidence from the public sector including police organisations emphasising the compliance and tick box mentality which pervades many processes including risk management (Lapsley, 2009). This suggests that potentially conceptual development of risk awareness and management at national, cultural and organisational level is the collective responsibility of government policy makers, risk regulators and large business organisations. The findings further emphasise that all organisations have risk management standards implemented in one form or another, for example health and safety policy, however risk management in relation to IT systems was not well communicated. In addition senior management was acknowledged to be ineffective in cascading knowledge of risk management appropriately to staff at other levels of the hierarchy. This has significant implications as communication and information flows are

acknowledged as critical elements to enhance risk awareness (ECHA, 2010; Science Wise ERC, 2009). Effectiveness is underlined by dynamic interactive communication with key groups and audiences (Infanti et al., 2013) suggesting that the organisations are missing critical opportunities to raise risk awareness. Another crucial finding is that organisations which should have 100% risk awareness and management in place such as government disaster departments and smaller private IT companies are the least aware about risk procedures. This underlines the potential need to understand the specific contexts in which risk awareness is practiced in order to tailor and develop appropriate risk awareness strategies.

The results show that a diverse level of knowledge in relation to risk awareness and management is evidenced in the Abu Dhabi Police Force. Gaps in awareness were evidenced as detailed knowledge of risk management was weak. A key result highlights the substantially widespread belief in the sole responsibility of the IT department to address risk and risk awareness reinforced by the majority view that it is not each employee's responsibility to assess organisational and IT systems risk. This perspective is potentially highly prejudicial to risk awareness as the findings in relation to risk awareness and the MERIT model emphasise the collective nature of risk responsibility and enhancing awareness. In terms of organisational practices to support risk awareness the results indicated a low level of implementation with limited extent of training while performance of risk assessment by the IT department was perceived as inconsistent and highly irregular.

Nevertheless the findings overall underline the major development in the AD Police over the past decade to address the security challenges faced by the country. This has witnessed progress towards a modernised e-police force working on a strategic, methodological and scientific basis. In conclusion, risk management is important for police organisations however the findings clearly show that they are yet to develop their risk management policies and programmes. Risk management should be integral to their strategy and operations and not implemented separately.

7.3 MERIT Model

A further key objective of the study focused on defining and exploring key elements of risk awareness based on a holistic theoretical framework composed of major areas of IT management. The central premise is that risk awareness levels in each of the areas of governance, compliance, enterprise, IT GRC, and risk management critically impact on the effectiveness of functions and the overall organisational success. Risk awareness within the MERIT model represents the central connecting underpinning dimension impacting on the effectiveness of the five other dimensions and which themselves have a significant iterative impact on risk awareness.

The findings from the Delphi Panel convened to identify and substantiate the components of the MERIT model demonstrate that a holistic approach is critical to enhancing IT risk awareness. The consensus expert view validated all five components of Governance, Compliance, Enterprise, IT GRC and Risk management within the MERIT IT systems risk awareness model. This confirms that individual and organisational risk awareness is dependent on these factors. The findings are consistent with Tarantino (2008) who emphasises governance, compliance and risk management as fundamental elements supporting risk awareness and Pohlman (2008) who argues the importance of all five factors.

The findings notably provide support for the integral role of governance in risk management, acknowledged to derive from its function in applying and enforcing the accountability and responsibility necessary in organisational processes and culture. The validation of governance as an important risk awareness variable is not unexpected as Cavalcanti (2014) notes that governance is a key tool for connecting the structures and processes of an enterprise. Evidence shows that the presence of strong governance can significantly enhance risk awareness and communication supporting an enterprise-wide culture of risk-awareness (EIU, 2013). Governance is therefore critical to embedding a risk culture which can impact the level and effectiveness of risk awareness and in turn impact effective management of risk. The findings show that application of governance potentially facilitates implementation of compliance as these two functions usually overlap each other due to organisational policy and regulatory requirements such as international standards for quality reporting. This suggests an interconnected element among the components in which the correct order of implementing the MERIT model would be governance → compliance → enterprise → IT GRC and over-

arching risk management process of identification – assessment – monitoring and control. This aligns with evidence from the EIU (2013) which shows that governance improves the coordination of functions essential to the promotion of risk awareness such as risk management and compliance.

This point further underlines that the relationship between the five dimensions of the MERIT model and risk awareness are highly intertwined. The results evidence a level of awareness of the interdependence of the risk factors in the MERIT model. Each contributes a perspective and focus in terms of raising awareness. Each component of this model is vital in promoting risk awareness and is in turn enhanced through enhanced risk awareness. On the one hand a key relationship between risk awareness and these dimensions is that awareness serves as a trigger in identifying and mitigating risks. At the same time the inherent processes can serve to enhance risk awareness that in turn feeds back into the cycle.

The findings point to the importance of enterprise-wide dimensions for promoting risk awareness on both an individual and organisational level. Risk awareness can enhance the ability of employees to differentiate between various risks, their contexts and their impacts. Promoting an enterprise approach to risk awareness further maximises the potential of tacit knowledge flows between individuals in different departments to promote understanding of issues and risks.

A number of studies provide significant support for the methods used to confirm and empirically validate the components of the MERIT IT risk awareness model. The use of risk management experts as in the Delphi method used in the present research is highly effective as it can combine both qualitative methods involving interpretative data and quantitative methods utilising statistical data. Al-Shehab (2007) investigated risk management methods, identification, control and mitigation in information systems projects to understand the reasons for the high number of information systems project failures involving experts and using a similar combination of qualitative and quantitative data. The proposed CorMod model contains strategies and techniques to model, analyse and simulate project factors relating to risk. Al-Shehab notes that, “expert opinion, together with a shared and highly visible model, plus the inherent facility for coherent group working, is shown to add

significantly to the capabilities of project stakeholders in understanding risk models, and therefore in mitigating risk."

Al-Shehab's (2007) use of experts concurs with the MERIT IT Risk model and its use of the Delphi Panel to derive quantitative measures of risk awareness. While identification and measurement of risk factors is necessary for risk management it is not sufficient and input from human expert views is significant. The MERIT risk management model identifies with a view to facilitating measurement of significant variables in enterprise risk management, but unlike other studies it deploys the Delphi method to use experts to provide a consensus view on risk management.

Ikram's (2000) study of information systems development projects found that claims in the literature about project management were not confirmed empirically. The study reveals that there is a lack of 'rigorous research into Risk Management' and risk management is not a common practice in information systems development projects, with little positive effect of risk management on practice. While Ikram's proposed 'socio-technical model' of risk management makes a valuable contribution by using multiple perspectives it is qualitative in nature. It traces the causes of risk to social and technical factors. The Delphi panel of experts in the present research empirically confirms that risk awareness is low among employees in enterprises, showing a value of zero (0). This kind of measurable value is more tangible and can be the impetus for immediate action to mitigate risk.

Qualitative knowledge of risk management improves our knowledge of the nature of risk but it does not improve our knowledge of how to measure and mitigate risk and provide a gauge on the levels of risk management achieved by organisations. The facility to measure risk awareness is a valuable contribution of the MERIT risk awareness model to the knowledge of risk management. Measurement is necessary to improve the quality of risk management through evidence.

Kutsch's (2005) study shows that risk awareness among IT systems development project managers is low, as, "project managers tended to deny, avoid, ignore risks and to delay the management of risk." He found that 'IT project managers were unaware of risks' and considered them beyond their scope of influence. More alarmingly, he found that "IT project managers preferred to let risks resolve themselves rather than proactively engaging with

them." In terms of practice, Kutsch's (2005) study is a quantitative explanation of risk management interventions in IT systems development projects and it does not provide the intervention tools.

7.4 Elements of Risk Awareness

This study also examined underlying cognitive, social, and psychological factors in relation to risk awareness to contribute towards conceptualisation of the MERIT model and IT risk awareness. In-depth qualitative interviews gathered data on risk awareness based on a conceptual framework adopted from the literature exploring the MERIT model and underpinning factors.

The findings emphasise that risk awareness is critically underpinned and influenced by a complex range of different elements on an individual and organisational level. These involve cognitive, social, cultural, emotional and psychological aspects in addition to the extent to which people understand a range of different types of risk. This points to the need to identify, assess and address these aspects in risk awareness implementations.

Firstly comprehensive awareness of different types of IT risk was found to be essential for a high level of risk awareness, suggesting the need to measure and assess this variable. The results however point to issues and challenges in maintaining relevant and up to date knowledge on the diverse and dynamically-changing IT threat environment. This is consistent with evidence from Kaspersky (2013) underlining the substantial daily emergence of new risks and threats spanning a diverse range of domains. Moreover an emphasis on the creation and upkeep of organisational systems is suggested to support the continuous updating of awareness and knowledge of IT risks. The findings highlight training on demand as a potential solution however the highly complex IT risk context implies that training alone may be inadequate and a range of complementary activities such as a focus on knowledge sharing and organisational learning could be significant for a comprehensive risk awareness. Quigly and Roy (2012) assert that information-sharing is a critical element in mitigating IT risks suggesting the potential benefits of this approach.

The results further underlined the essential importance of differentiating between critical and common risks as part of effective overall risk awareness. This insight is supported by studies which show that risk management practices frequently emphasise identification and mitigation of critical risks (Kaplan and Mikes, 2012), suggesting that measuring how well common and critical risks are understood within an organisation is an important aspect of risk awareness and should be included in risk awareness conceptualisations and practice. The findings suggest however that this aspect is not well understood at an organisational level given the lack of processes in place to ensure that awareness of common and critical risks is high through continuous identification. This further implies potential weaknesses in governance as best practice shows that measurement and accountability for the status of critical risks is an important aspect of IT governance (NCC, 2005).

A key result indicated that the organisations were impacted by the need to consistently update risk awareness in the light of new and novel risks. However effective mechanisms for promoting this aspect appeared to be lacking as results show this aspect to be weak in the organisations. Allan and Beer (2006) underline that this is potentially a critical omission as greatest susceptibility to risk was found in areas of limited knowledge where high impact but unexpected risks arose. This emphasises that increased understanding of new or novel risks is significant for minimising vulnerability. The result may partially be explained by the acknowledged weaknesses in knowledge flows from external contacts and sources which appear not to be fully optimised to enhance awareness of new and emerging risks.

The evidence points to the importance of flexible and diverse sources of knowledge for enhancing risk awareness, implying the significance of measuring this variable within a robust and comprehensive model. This is potentially because external knowledge flows can stimulate awareness around significant environmental changes impacting IT risks or introducing novel ones (Anderson, 2005). However the findings suggest issues in obtaining diverse knowledge which, when considered in the context of enterprise risk management, implies a significant gap in risk assessment supporting enhanced risk awareness. Hempe (2011) emphasises that knowledge flows are generally neglected within the design of processes, underlining further the need for a specific focus on this aspect. The findings additionally point to the importance of creating and maintaining networks of relationships and contacts with external users and suppliers which can enhance knowledge flows to support improved risk awareness. Theories on absorptive capacity and organisational learning stress

the significance of strong positions within relationship networks for deepening and widening knowledge in relation to the external business environment (Koka and Prescott, 2002).

Embedding risk awareness within the MERIT model both in relation to informal and informal processes is a key finding arising from this study. In many ways the informal inter and intra organisation and departments linkages provide diverse sources of inputs for risk awareness. There were views that responsibility for risk awareness can be placed on individual employees and teams. The suggestion is that if it is free flowing then new risks can be identified and the organisation is not regimented in ticking off existing already identified risks.

Risk awareness was also found to fundamentally incorporate a number of different cognitive processes acknowledged to each have their own importance in holistic perspectives. This provides support for the importance of the cognitive element within the proposed risk awareness model. The results are supported by theory which highlights cognitive processes as fundamental elements of models of risk awareness (Endsley, 1995; Wilde, 1982). Empirical work by Belle and Banet (2012) highlights the effectiveness of measuring these variables for forming a robust view of levels of risk awareness and differences between individuals. It has been argued by Horswill and McKenna (2004) that hazard detection or a lack of it is the most important factor in risk events however in contrast Belle and Banet (2012) strongly emphasise hazard perception as the first step in a more complex process of diagnosing and decision-making asserted to underpin risk awareness. This implies that adequate, timely and accessible information and guidelines to underpin cognitive perception and evaluation of risk could be essential in enhancing risk awareness.

A key finding further indicates that enhanced risk awareness involves the utilisation of common sense, alertness and engaging a presence of mind on the part of individuals to cues in their environment, reinforcing support for the cognitive role in risk awareness. This was perceived as an essential part of the management of unexpected or unanticipated risks and for establishing pro-active risk awareness and behaviour. The finding is consistent with studies which have underlined the importance of presence of mind and common sense in enhancing risk awareness (Borys 2007; Weick et al., 1999). Hopkins (2005) shows that workers which are risk-aware indicate higher propensity for noticing more risks and potential hazards and are more likely to report them. Weick et al., (1999) also highlights the significance of this

aspect for promoting pro-active behaviour in relation to risk. Weick and Sutcliffe (2001) further point to strong cultural underpinnings for enhancing risk awareness through collective presence of mind suggesting that this aspect may be promoted through organisational values, norms and expectations. This points to the potential role of organisational risk culture in supporting collective mindfulness.

Socio-cultural factors were further found to be critical for shaping risk awareness. In particular organisational culture, values and norms were fundamental influences on risk awareness, consistent with a range of studies which have asserted the importance of organisational culture in this context (Karyda et al., 2004; Schein, 1984). The result underlines the importance of understanding and assessing the role of organisational cultural factors as essential components of IT risk awareness models and further reinforces the need for an enterprise-wide risk awareness approach. This is supported by Hopkins (2007) who asserts that cultural and enterprise-wide approaches to risk including risk-awareness programmes are not solely dependent on individual risk awareness but also on organisational systems which promote individual risk-awareness (Hopkins, 2007). Rhee et al., (2012) highlight the challenge for changing individual perceptions and behaviours in relation to risk. The findings suggest that organisational culture in defining risk values, norms and expectations could be a significant tool for addressing the need to change behaviour. Moreover potentially organisational culture links to and could positively influence a range of other variables within the risk awareness model including psychological biases.

The findings showed a significant consensus in relation to the impact of subjective perceptions on IT risk awareness underlining the validity and relevance of measuring these aspects within a risk awareness model. This is consistent with a number of studies which have indicated that subjective biases can lower or override an individual´s risk awareness (Schneier, 2004; Breakwell, 2007; Hogarth, 2011). Studies imply the criticality of managing perceptual biases in risk awareness approaches as they can exacerbate risk-taking (Adams 1999; Erenberg, 2005) and undermine preventive actions and precautionary behaviours (Schwarzer 1994; Helweg-Larsen and Shepperd 2001). Therefore, the results point to the necessity for consideration of psychological factors to optimise risk awareness however the diverse range of biases noted stresses the significant complexity involved in establishing metrics to assess this aspect. Nevertheless the role of governance, a central variable in the risk awareness model, is shown to be important for countering subjective risk perceptions and

factors. This is further consistent with general deterrence theory (Straub and Welke, 1998) which can potentially underpin a governance approach to addressing perceptual biases.

A further major result shows that employees were generally aware of the IT risks to the organisation and to other departments and this influenced a more aware and cautious approach to taking risks. This suggests that an important element of maximising risk awareness and encouraging appropriate security behaviour is a thorough apprehension by employees of the wider risks and consequences to other employees, departments or functions and to the organisation as a whole. The results are consistent with theories on the influence of social bias in which individual risk perceptions are higher in relation to others´ risks (Schneier 2008) and underline the effect of socio-cultural factors on individual risk awareness. This provides support for consideration and evaluation of this aspect.

In conclusion the study has presented an empirically validated model of risk awareness involving five separate factors which address it from different perspectives to provide a holistic view and the ability to evaluate it in these different contexts. The findings highlight the interdependency of the factors and their iterative character. Therefore IT risk awareness can promote governance however governance needs to be addressed in ways which promote risk awareness. This study also shows that risk awareness is a complex phenomena which needs to be addressed in a more comprehensive and precise way through examining and evaluating the different cognitive, psychological, behavioural and emotional elements and influences which underpin it. This last point emphasises that effective risk awareness and risk management critically involves understanding and managing people and their awareness.

7.5 Conclusions

This research explored the importance of risk awareness amongst all levels of employees to understand its contribution to enterprise risk management. The findings point to a number of significant conclusions which can be applied in the context of enhancing the risk awareness of the AD Police. Firstly understanding of risk management appears to be limited within the UAE and there is significant scope to maximise the practice of IT risk management in relation to the understanding, usage and level of risk awareness. Moreover communication of risk management in relation to IT systems is ineffective and senior management is limited in cascading knowledge of risk management appropriately to staff. This has significant

implications as communication and information flows are critical elements to enhance risk awareness. A holistic approach is indicated as critical to raising IT risk awareness suggested by the validation of all five components of Governance, Compliance, Enterprise, IT GRC and Risk management within the MERIT IT systems risk awareness model. A further conclusion underlines the iterative and interdependent nature of the various components emphasising the inclusion of all elements in any risk awareness implementation. Finally, risk awareness is critically underpinned and influenced by a complex range of different elements involving cognitive, social, cultural, emotional and psychological aspects in addition to the extent to which people understand a range of different types of risk. The MERIT model provides significant opportunity to identify, assess and address these elements.

Chapter 8: Conclusion

8.1 Introduction

This study is concerned with exploring and understanding IT risk awareness and establishing a conceptual understanding of risk awareness. Chapter 1 introduces the background and context of the study and presents the research problem, the aims and objectives of the study and the methodology used. The contribution of the research to greater understanding of risk awareness is also discussed. Chapter 2 provides an interdisciplinary review of the literature on risk and risk management as the underlying basis for conceptualising risk awareness and supporting the formulation of a conceptual framework for IT systems risk awareness. Chapter 3 addresses IT systems risk awareness conceptualising the topic and identifying key findings and gaps in the literature. The findings from the review informed the conceptualisation of the MERIT model of IT risk awareness presented at the end of the chapter. Chapter 4 details the research methodology adopted to address the research goals and provides a rationale and justification of the research approach, strategy and methods. Chapter 5 presents the results of quantitative surveys and in-depth qualitative interviews investigating risk management and awareness in the ADP and UAE organisations. These findings inform the evaluation of current IT risk management practices within these entities. The qualitative evidence further confirmed the importance of the MERIT model for conceptualising risk awareness. Chapter 6 presents the results of a Delphi panel to validate the MERIT IT systems risk awareness conceptual model, indicating support for the importance of each component of the proposed model. Chapter 7 discusses the findings of the study. The results are linked with existing theory and research and the potential reasons, meaning, and implications of the results in the context of the study objectives are critically analysed. Chapter 8 concludes the project presenting a summary of key findings in addition to critical recommendations and study limitations and further research.

This research is founded on the premise that IT risk awareness among individuals in all levels of the organisation is critical and involves consideration of human and social factors. A **M**anag**e**ment of **R**isk Awareness in **R**elation to **I**nformation **T**echnology (MERIT) model is investigated. Five dimensions (governance, compliance, enterprise, IT GRC, risk Management) represent five major areas of IT management which have become increasingly dependent on new awareness of risk, the sixth dimension. The research aimed to evaluate

current practice in IT risk awareness in police forces and explore what police forces in the UAE can learn from the best practices of other UAE public and private enterprises. The development of a new holistic framework of IT risk awareness supporting IT risk management was a key objective. Quantitative and qualitative data was collected to achieve the research objectives utilising three main techniques of structured survey, a Delphi method and in-depth interviews. This research explored the importance of risk awareness amongst all levels of employees to understand its contribution to enterprise risk management.

8.2 Summary of Key Findings

A key objective of this study was to evaluate current IT risk management practices in the Abu Dhabi Police and selected UAE organisations. The findings indicate a lack of formalised risk management processes and a lack of IT risk awareness. Although the ADP particularly demonstrated these weaknesses this was also reflected to a lesser extent in other UAE organisations. The results show that a diverse level of knowledge in relation to risk awareness and management is evidenced and detailed knowledge of risk management was weak in addition to low awareness of policies and guidelines. Moreover IT risk awareness and management was perceived as solely the domain of IT departments and not as a collective responsibility. This finding underlined the importance of providing a conceptual framework for evaluating risk awareness as the basis for maximising or embedding risk awareness interventions.

This study also aimed to develop a new conceptual model of IT risk awareness. The findings showed that risk awareness levels in each of the MERIT areas critically impacts on the effectiveness of functions and the overall organisational success. These dimensions present a holistic frame of reference for exploring risk awareness. Support for the significance of all five components of Governance, Compliance, Enterprise, IT GRC and Risk management in relation to risk awareness is further provided by the findings. Significant expert consensus affirmed that it is appropriate and important to examine risk awareness in relation to these elements. The results highlighted the interdependency and iterative interactions between these dimensions and the key role of governance in facilitating risk awareness and other elements.

The conceptualisation of risk awareness was further underpinned by findings indicating the significance of specific aspects and elements which impact on overall risk awareness. A range of different elements involving cognitive, social, cultural, emotional, cognitive and psychological factors were found to influence the degree of risk awareness. Findings indicated that socio-cultural factors involving organisational culture, values and norms, in addition to a range of subjective perceptual biases are critical for positively or negatively influencing individual risk awareness. The importance of flexible and diverse sources of knowledge for enhancing risk awareness was also underlined. Overall, this study supports two key conclusions. Firstly, that a holistic approach to risk awareness that interrelates the five dimensions in the MERIT model maximises individual and organisational capability for risk identification and risk management. Secondly, a number of components of risk awareness should be evaluated to assess the impact on overall risk awareness.

This study indicates that the MERIT approach to risk awareness provides a significant frame of reference to identify, assess and address these factors through a holistic conceptualisation involving all elements of IT management and risk management supporting the fundamental social and human perspective within IT risk awareness.

8.3 Recommendations

Several key recommendations are presented arising from the findings. Firstly, there is evidence to consider a strategic approach to risk awareness to develop an integrated cross-cutting approach to risk management which develops processes to generate linkages between the five MERIT dimensions.

The results suggest a basic level of risk awareness and management with issues in either implementation or communicating risk mechanisms to employees. The level of risk awareness and knowledge amongst the employees at AD Police IT Department needs to improve. This establishes the need for increased resource allocation from top management of AD Police so that employees can be trained effectively to understanding the scale of risk effects on the organisation and how to identify, assess and mitigate risk through individual or team decision making. Hence, governance should reveal the risks to all involved in the process and have it as a transparent element. Organisations with good governance can focus on increased awareness of risk to achieve their objectives and goals.

Specific strategic measures should be considered under each of the dimensions to maximise risk awareness and to address factors inhibiting its enhancement. Organisations should consider adopting an approach to measuring risk awareness that captures different elements. This should combine with the development of instruments or processes for measuring risk awareness based on the elements identified in this study. Integration of such processes into existing HR including performance appraisals and learning and development potentially ensure a cost-effective approach to align measures to maximise risk awareness. This can be innovatively addressed by making adjustments to existing practices. A HR manager suggested that one of the best ways to raise enterprise-wide understanding of risk is to offer job rotations. This address a number of strategic HR issues but also promotes knowledge exchange. Employees returning from different rotations can share knowledge and experiences and raise awareness on other business and work contexts.

Enterprise-wide risk awareness can be adopting using collaborative and cross-team practices and processes that promote knowledge sharing. The adoption of e-learning and social media systems can be integrated to foster learning ecosystems and informal learning which simultaneously address development needs and maximises risk awareness through knowledge sharing and social learning.

The other important factors embedded within risk awareness and its fundamental dimensions are training skills, feedback given by employees and time taken to plan, implement and learn the risk management by employees. The risk awareness quality and accuracy for organisation's risk reduction and increased value addition, depends largely on response or reaction time taken up by the systems, structure and process of the organisation. Addtionally, the concept of risk in its various forms at different hierarchical levels is a complex domain in itself. Therefore, training and implementation with appropriate communication is required to infuse accountability and responsibility in each employee in relation to risk management.

Awareness needs to be embedded early at the start of a job and evaluated over time. This potentially involves orienting new employees towards risk awareness ensuring that they incorporate a critical understanding of IT risks and response obligations through induction and training of response resources. This enhances organisational learning and the production of knowledgeable, aware employees. Nevertheless risk awareness orientation should not be limited to the start of jobs but be encouraged throughout employees´ careers. This could

involve shifting the focus of risk awareness into the workplace with communities of practice a focal point for behaviour and culture change and learning. Further techniques such as story-telling on safety should be utilised to promote the growth of worker common sense and mindfulness in relation to IT risk.

The findings suggest that there is an immediate need of risk awareness and risk management procedure implementation. This should start with a governance mechanisms plan, as many employees did not fully appreciate or understand the extent of risk awareness.

8.4 Limitations and Further Research

There are several limitations to this study which should be borne in mind in relation to the results and interpretations. The lack of probability sampling is a limitation for this study in terms of selection of quantitative data selection. This may mean that it fails to withstand positivist scrutiny and suggests potential bias in the findings towards ADP and those organisations in this study which limits the generalisation of the findings of the study. It should be noted that the quantitative data drawn from the Delphi method was primarily aimed to provide quantitative support for the significance of the MERIT dimensions in relation to risk awareness.

Further the data from the ADP reflects data from a single police organisation. This limitation is less of an issue in relation to the qualitative data which has enabled the exploration of in-depth individual and group interpretations. While it is not possible to determine whether the results either qualitative or quantitative reflect the wider population of organisations the findings have contributed to an understanding of the risk awareness factor underpinning IT risk identification and risk management. Even so the context of this study means the findings are limited to the context of both the ADP and UAE organisations. Cultural and institutional factors can vary significantly between Arab countries and between other countries. Further research would be required to gather data on risk awareness in other contexts.

There is also limitation with the design of the study in relation to researcher bias which in the qualitative aspect of this study can reflect the interpretation of the researcher's subjective perspective. While the qualitative interviews provided opportunity to gather rich in-depth data on risk awareness factors the data collection and analysis was subject to the researcher´s subjective analysis. Adoption of interviews and focus on one police organisation limits the

findings. This limitation is common to qualitative studies but should be borne in mind given the relative inexperience of this researcher. Finally, it is important to note that this study is primarily a cross-sectional study focused principally on Abu Dhabi Police and a subset of UAE organisations sampled from across a range of sectors.

Further empirically-based research may be undertaken to establish the validity of critical components of risk awareness. This can examine the relative impact of a wide range of variables on risk awareness. In particular structural equational modeling can be applied to test the relationship between different variables on risk awareness. Further research can also be undertaken in relation to the nature of risk awareness in the context of the five MERIT dimensions outlined in this study. Further research may also be explored in relation to the impact of different learning interventions on maximisation of risk awareness. This can extend to an understanding of absorptive capacity, cognitive structures and network embeddedness which can be applied to develop theoretical understanding of how risk awareness can be enhanced.

The IT Risk Awareness elements proposed in this work can be used to assess individuals' and organisations' IT risk awareness but requires further research into the design of instruments for effectively measuring and evaluating risk awareness. The MERIT IT risk awareness model provides tangible measures and values of pertinent variables that define risk awareness, contributing to the overall enterprise risk management. However, such values and measures need to be interpreted in the social context of organisational work. How these metrics can be actually implemented socially to improve risk awareness is still open to further research.

8.5 Conclusion

Current business environments are characterised by a wide range of factors and issues which combine to create an unprecedented level of uncertainty and exposure to risks in IT management and all areas of strategic and operational activities. However IT risk awareness presents both a problem and an opportunity to achieve effective IT risk management. This context creates an imperative for conceptualising risk awareness to account for the intensity, diversity and complexity of IT risks to ensure a heightened level of awareness.

The originality of the research lies in the examination of how risk awareness and risk management can fit with IT systems risk management and the risk awareness of people who manage and operate them. This makes a significant contribution to enterprise risk management through risk awareness. The research contributes to knowledge in relation to a conceptualisation of risk awareness with a view to evaluating these aspects as an integral part of organisational risk management strategies. The outcomes of this research will enable enterprises to improve individual risk awareness to enhance the effectiveness of enterprise risk management. The MERIT risk awareness model can be applied in practice to obtain tangible measures of enterprise risk management. The IT Risk Awareness dimensions proposed in this work can be used to assess individuals' and organisations' IT risk awareness, but the question of how to motivate employees to comply with information security guidelines is still a rich topic of research. The MERIT IT risk awareness model provides tangible measures and values of pertinent variables that define risk awareness, contributing to overall enterprise risk management. However, such values and measures need to be interpreted in the social context of organisational work. How these dimensions and evaluation can be implemented socially to improve risk awareness is still open to further research.

References

Abu Dhabi Police, (2008). *About Us*. [online] Available at: <http://www.adpolice.gov.ae> [Accessed 15 July 2014].

ACCA, (2007). *Answers*. [online] Available at: <http://www.accaglobal.com/content/dam/acca/global/PDFstudents/2012/dec2007ans.pdf > [Accessed 25 November 2014].

Adam, B, (2000). *The Risk Society and Beyond*. London: Sage.

Adams, J, (1999). *Cars, Cholera, and Cows: The Management of Risk and Uncertainty*. Cato Institute Policy Analysis, No. 335.

Agrawal, M., Campoe, A. and Pierce, A, (2014). *Information Security and IT Risk Management*. Hoboken: John Wiley & Sons.

Al-Fehaid, A. M. (2003). *An Investigation of the Influence of Information Technology on Audit Risk in Saudi Arabia*. PhD Thesis. Loughborough University, UK.

Alreck, P. and Settle, R, (1995). *The Survey Research Handbook*, 2nd edition. New York: McGraw-Hill.

Al-Shehab, A, (2007). *Causal and Cognitive Mapping Methods for the Identification of Risk In Information System Development Projects.* PhD Thesis. University of Brighton UK.

Alviunessen, A. and Jankensgård, H, (2009). Enterprise Risk Budgeting: Bringing Risk Management Into the Financial Planning Process. *Journal of Applied Finance*, 19(1/2), p. 178-190.

Andersen, T.J, (2005). *A Strategic Risk Management Framework for Multinational Enterprise*. SMG Working Paper No. 3/2005. [online] Available at: <http://openarchive.cbs.dk/bitstream/handle/10398/7426/smg%20wp%202005-003.pdf?sequence=1> [Accessed 25 November 2014].

Andress, J, (2014). *The Basics of Information Security*, 2nd Edition. Oxford: Syngress.

Ansell, J. and Wharton, F, (1992), *Analysis, Assessment and Management*. John Wiley & Sons: Chichester.

AOL/NCSA, (2004). *AOL/NCSA Online Safety Study*. American Online and the National Cyber Security Alliance. [online] Available at: <http://www.bc.edu/content/dam/files/offices/help/pdf/safety_study_2005.pdf>[Accessed 25 November 2014].

Aon, (2009). *The Definitive Report on Risk.* [online] Available at: <http://insight.aon.com/?elqPURLPage=3907> [Accessed 15 July 2014].

Arend, R. J, (2012). Bursting Bubbles, What the internet Could Have Meant to the Strategic Management Academia. *Journal of Management Inquiry*, 15 (4), p. 372-382.

Assailly, J-P., (2012). *The Psychology of Risk*. Canada: Nova Science Publishers.

Aven, T. and Renn, O, (2010). *Risk Management and Governance: Concepts, Guidelines and Applications*. London: Springer Science & Business Media.

Bailey, K. D, (1994). *Typologies and Taxonomies*. London:Sage.

Bakker, K., Boonstra, A. and Wortmann, H, (2011). Risk Management Affecting IS/IT Project Success Through Communicative Action. *Project Management Journal*, 42 (3), p. 75 – 90.

Banks, J., Carson, J., Nelson, B. and Nicol, D, (2005). *Discrete-Event System Simulation*. London: Pearson.

Baskerville, R, (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *Eur J Inf Sys*, 1(2), p.121 - 30.

Bauman, Z, (2007). Collateral Casualties of Consumerism, *Journal of Consumer Culture*, 7(1), p.25–56.

Bayaga, A. and Moyo, G, (2009). An Investigation into the Relevance and Applicability of University-wide Risk Awareness: Effect of Risk Policies and Procedures. *The Journal of International Social Research*, 2(9).

Beck, U, (1992). *Risk Society: Towards a New Modernity*. London:Sage.

Beck, U, (2000). Risk Society Revisted: Theory, Politics and Research Programme. In: B, Adam., (2000). *The Risk Society and Beyond*. London: Sage.

Benaroch, M., Lichtenstein, Y. and Robinson, K, (2006). Real Options in Information Technology Risk Management: An Empirical Validation Of Risk-Option Relationships. *MIS Quarterly*, 30(4), p. 827-864.

Benjamin, D.J., Brown, S.A. and Shapiro, J.M, (2006). *Who is "Behavioral"? Cognitive Ability and Anomalous Preferences.* Levine's Working Paper Archive.

Bernstien, P. L, (1998). *Against the Gods, The Remarkable Story of Risk*. New York: John Wiley.

Bickman, L. and Rog, D.J, (2008). *The SAGE Handbook of Applied Social Research Methods*. London: SAGE Publications.

Blaikie, N, (1993). *Approaches to Social Enquiry*, 1st edition. Cambridge: Polity Press.

Blaikie, N., 2000. *Designing social research*, 1st edition. Cambridge: Polity Press.

Boeham, B. W, (1991). Software Risk Management Principles and Practices. *IEEE Software,* 8 (1), pp. 32-41.

Borodzicz, E. P., (2005). *Risk, Crisis & Security Management*. Chichester: John Wiley & Sons Ltd.

Bowen, P L, (2006). *Risk Management in Project Organisation*. USA: Unsw Press.

Bowen, P. L., Cheung, M. D. and Rohde, F. H, (2007). Enhancing IT Governance Practices: A Model and Case Study of an Organisation's Efforts. *International Journal of Accounting Information Systems*, 8, p.191 – 221.

Breakwell, G.M, (2007). *The Psychology of Risk*. Cambridge: Cambridge University Press.

British Standard 25999, (2006), *Business Continuity Management.* Part 1, Code of Practice.

Broder, J. F, (2000), *Risk Analysis and the Security Survey*, 2nd edition. USA: Butterworth-Heineman.

Brunschot, E. G. V. and Kennedy, L. W, (2008). *Risk Balanace & Security*. London: Sage.

Bryman, A. and Bell, E, (2007). *Business Research Methods*. 2nd edition. Oxford: Oxford University Press.

Burrell, G. and Morgan, G, (1979). *Sociological Paradigms and Organisational Analysis*. London: Heineman.

Cavalcanti, J, (2014). *Effects of IT on Enterprise Architecture, Governance, and Growth*. Hershey: IGI Global.

Ceraolo, J. P, (1996). Penetration Testing Through Social Engineering. *Information Systems Security* ,4(4).

Channel 4, (2012). *New Police Corruption Alleged in Secret Report*. [online] Available at: <http://www.channel4.com/news/new-police-corruption-alleged-in-secret-report> [Accessed 15 July 2014].

Chapman, C. and Word, S, (2002) *Managing Project Risk and Uncertainty*. Chichester: John Wiley & Sons Ltd.

Checkland, P, (1981). *Systems Thinking, Systems Practice*. Chichester: John Wiley & Sons Ltd.

Chia, R, (2002). The Production of Management Knowledge: Philosophical Underpinnings of Research Design. In: D. Partington., (ed). 2002. *Essential Skills for Management Research,* 1st edition. London: Sage Publications Ltd.

Christensen, C. M. and Carlile, P. R, (2009). Course Research: Using the Case Method to Build and Teach Management Theory. *Academy of Management Learning and Education*, 9 (2), p.240-251.

Christopher, J, (2010). Corporate Governance – A Multi-Theoretical Approach to Recognizing The Wider Influencing Forces Impacting on Organizations. *Critical Perspectives on Accounting,* 21, p. 683 – 695.

Cohen, L., Manion, L. and Morrison, K, (2013). *Research Methods in Education*, 7th edition. Abingdon: Routledge.

ContinuityCentral.com, (2012). The international business continuity portal. [online] Available at: <http://www.continuitycentral.com/> [Accessed 15 July 2014].

Cooper, D.R. and Schindler, P.S, (2003). *Business Research Methods*. London: McGraw-Hill/Irwin.

COSO, (2004). Enterprise Risk Management-Integrated Framework, Executive Summary. *National Committee of Sponsoring Organisations.* New York: The Committee of Sponsoring Organisation of the Tradeway Commission.

Coyle, B, (2002). *Risk Awareness and Corporate Governance.* London: Financial World Publishing.

Coyle, B, (2004). *Risk Awareness and Corporate Governance*, 2nd edition. Canterbury: Institute of Financial Services.

CSI, (2011). *Computer Crime and Security Survey 2011/12.* <http://gocsi.com/survey.>

D'Arcy, J., Hovav, A. and Galletta, D, (2008). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research Articles in Advance*, pp. 1–20.

Data, (2006). Data and Electronic Records, Management: Best Practices, Technology Standards. *Texas Department of Information Resources, ACE Data and Electronic Records Management Domain*, USA.

Davis, F.D, (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems : Theory And Results*. PhD Thesis. Massachusetts Institute of Technology, Sloan School of Management.

Davis, P. J. and Hersh, R, (1999). *The Mathematical Experience*. London: Mariner Books.

Delavande, A, (2008). Measuring Revisions to Subjective Expectations. *Journal of Risk Uncertainty*, 36, p.43-82.

DeLucciaIt, J. J, (2008). *Compliance and Controls: Best Practices for Implementation*. Hoboken: John Wiley & Sons.

Denscombe, M, (2007). *The Good Research Guide*, 3rd Edition. London: Open University Press.

DeSteno, D, Petty, R. E, Wegner, D. T, and Rucker, D. D. (2000). Beyond valence in the perception of likelihood: The role of emotion specificity. *Journal of Personality and Social Psychology*, 78 (3), p.397-416.

Devaki, R. and Thorvald, H, (2010). Applying an Organizational Learning Perspective to New Technology Deployment by Technological Gatekeepers: A Theoretical Model and Key Issues for Future Research. *Information Systems Front*, 12, p.287–297.

Dey, P. K., Kinch, J. and Ogunlana, S. O, (2007). Managing Risk in Software Development Projects: A Case Study. *Industrial Management and Data Systems*, 107 (2), p. 284 – 303.

Dixon, R, Marston, C. and Collier, P, (1992). Report on the Joint CIMA and IIA Computer Fraud Survey. *Computers & Security,* 11 (4), p. 307-313.

Douglas, M, (1978). *Cultural Bias*. Occasional Paper no. 35. Royal Anthropological Institute of Great Britain and Ireland.

Dunkerley, D. and Samuelle, T. J, (2014). *Mike Meyers' CompTIA Security+ Certification Passport*, 4th Edition. New York: McGraw-Hill Osborne Media.

Dutta, A. and Roy, R, (2003). The Dynamics of Organizational Information Security. In: S.T. March, A. Massey, and J.I. DeGross, eds, (2003). *Proceedings of the Twenty Fourth International Conference on Information System*, p. 921 e 927.

Easterby-Smith, M., Thorpe, R. and Jackson, P, (2012). *Management Research*, 5th edition. London: Sage.

Economist Intelligence Unit, (2013). *Closing the Communication Gap: How Institutional Investors Are Building Risk-Aware Cultures*. [online] Available at: <http://www.economistinsights.com/sites/default/files/downloads/Communication_Gap__WEB_May8_FINAL.pdf>[Accessed 25 November 2014].

Eloffr, J.H.P., Labuschagne, L. and Badenhorst, K.P, (1993). A Comparative Framework for Risk Analysis Methods. *Computers & Security,* 12(6), p. 597-603.

Emerson, S.A., Reising, T.J. and Britten-Austin, H. G, (1987). *Workload and Situation Awareness in Future Aircraft*. SAE Technical Paper (No. 871803). Warrendale, PA: Society of Automotive Engineers.

Emery, F. and Trist, E, (1965). The Causal Texture of Organizational Environments. *Human Relations*, 18 (1), p. 21-32.

Endsley, M. R. and Garland, D. J, (2000). *Situation Awareness Analysis and Measurement*. London: CRC Press.

Endsley, M. R. and Robertson, M. M, (2001). *Building A Framework For Situation Awareness.* [online] Available at: <http://www.satechnologies.com/Papers/pdf/SATrainingchapter.pdf>[Accessed 25 November 2014].

Epich, R. and Persson, J, (1994). A Fire Drill for Business, Information Strategy. *The Executive's Journal,* p. 7-44.

Epstein, S, (1994). Integration of the Cognitive and Psychological Unconscious. *American Psychologist*, 49, p. 709-724.

Erenberg, E, (2005). What Type of Disputes are Best Suited for Alternative Dispute Resolution: An Analysis in the Space of the Odds of Litigation. In: *Proceedings of the Fourth Annual Meetings of Israeli Law & Economics Association* (ILEA); 2005. [online] Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=731346> [Accessed 25 November 2014].

Eriksen, C. W, (1962), *Behavior and Awareness.* Durham: Duke University Press.

Eriksson, P. and Kovalainen, A, (2008). *Qualitative Methods in Business Research*. 1st edition. London: Sage Publications.

Eurich, M, Oertel, N. and Boutellier, R, (2010). The Impact of Perceived Privacy Risks on Organisations' Willingness to Share Item-Level Event Data Across The Supply Chain. *Electronic Commerce Research,* 10, p. 423-440.

Eves, H, (1983). *Great moments in Mathematics (before 1650).* The Mathematical Association of America.

Focus, (2012). *Top 10 Largest Databases in the World*. [online] Available at: <http://www.focus.com/fyi/10-largest-databases-in-the-world/> [Accessed 15 July 2014].

Foltz, C. B, (2000). *The Impact of Deterrent Countermeasures Upon Individual Intent to Commit Misuse: A Behavioral Approach*. PhD Thesis. University of Arkansas, Fayetteville.

Forcht, K. A. (1994). *Computer Security Management*. Boyd & Fraser,Danvers, MA.

Fraser, J. and Simkins, B, (2010). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Hoboken: John Wiley and Sons.

Gerber, M. and von Solms, R. (2005). Management of Risk in the Information Age. *Computers and Security*, 24(1), p. 16-30.

Gibson, S. D, (2003). The Case for Risk Awareness. *Security Journal*, 16, p. 55–64

Goodhue, D, L. and Straub, D. W, (1989). Security Concerns of System Users: A Proposed Study of User Perceptions of the Adequcey of Security Measures. *In the Proceedings of the 21st Hawaii International Conference on System Science (HICSS)*, Kona, HA.

Goodhue, D. L. and Straub, D. W, (1991) .Security concerns of systems users: A study of perceptions of the adequacy of security measures. *Information & Management*, 20 (1), p.13-27.

Gottschalk, P, (2010). Knowledge Management Technology for Organised Crime Risk Assessment. *Information Systems Frontier*, 12, p. 267-275.

Graham, J. and Kaye, D, (2006). *A Risk Management Approach to Business Continuity, Aligning Business Continuity with Corporate Governance*. New York: Rothstein Associates Inc.

Guehlstorf, N.P, (2004). *The Political Theories of Risk Analysis*. London: Springer Science & Business Media.

Haber, J, (2011). The Problems of Quantifying Risk. *Journal of Applied Business and Economics*, 12(2), p. 61-63.

Haight, F.A, (1986). Risk, Especially Risk of a Tragic Accident. *Accident Analysis Prevention* 18, p.359–66.

Haimes, Y. Y, (1998). *Risk Modeling, Assessment and Management*. Chichester: John Wiley & Sons.

Hampton, J, (2014). *Fundamentals of Enterprise Risk Management*, 2nd Edition. New York: AMACOM

Hancock, J, (2001) *Environmental Risk Management and Your Business*. London: The Stationary Office.

Harkins, M, (2012). *Managing Risk and Information Security: Protect to Enable*. UK: Apress.

Harwood, K., Barnett, B. and Wickens, C, (1988). Situational Awareness: A Conceptual and Methodological Framework. In: *Proceedings of the Psychology in the Department of Defense Eleventh Symposium* (Tech. Report No. USAFA-TR-88-1, pp. 316-320). Colorado Springs, CO: US Air Force Academy.

Hatch, M. J. and Cunliffe, A. L, (2006). *Organization Theory*, 2nd edition. Oxford: Oxford University Press.

Helweg-Larsen, M. and Shepperd, J.A, (2001). Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A review of the literature. *Personality and Social Psychology Review*, 5, p. 74 - 95.

Hempe, E.M, (2011). *Knowledge Flows in Service Design - A Framework*. 44th Hawaii International Conference on Systems Science (HICSS-44 2011), Proceedings, 4-7 January 2011, Koloa, Kauai, HI, USA.

Hevner, R., March, S. T., Park, J. and Ram, S, (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28, p. 75-105.

Hickson, R.J. and Owen, T.L, (2015). *Project Management for Mining: Handbook for Delivering Project Success*. Colorado, US: SME.

Hiles, A. and Barnes, P, (1999). *The Definitive Handbook of Business Continuity Management*. Chichester: John Wiley & Sons Ltd.

Hillson, D, (2006). *The Risk Management Universe*. London: British Standards Institution.

HM Treasury, (2004). *The Orange Book: Management of Risk - Principles and Concepts*. [online] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf>[Accessed 25 November 2014].

Hoffer, J. A. and Straub, D. W, (1989). The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review*, 30(4).

Hogarth, R. M, Portell, M., Cuxart, A. and Kolev, G. I, (2011). Emotion and reason in everyday risk perception. *Journal of Behavioural Decision Making*, 24, p. 202-222.

Hogarth, R. M., Portell, M. and Cuxart, A, (2007). What risks do people perceive in everyday life? A perspective gained from the experience sampling method (ESM). *Risk Analysis*, 27(6), p.1427-1439.

Hood, C. C, (1992). Risk Management. In: Royal Society Study Group (2002). *Risk, Analysis, Perception and Management*, p. 135-192. London: The Royal Society.

Hopkin, P, (2013). *Risk Management*. London: Kogan Page.

Hopkin, P, (2014). *Fundamentals of Risk Management*, 3rd Edition. London: Kogan Page.

Horlick-Jones, T, (2007). On the Signature of New Technologies: Sociality, Materiality and Practical Reasoning. In: Flynn, R. and Bellaby, P. eds. *Risk and the Public Acceptance of New Technologies,* pp.41-65. Basingstoke: Palgrave Macmillan.

HSE, (2006). *Risk Assessment: A Brief Guide to Controlling Risks in the Workplace.* [online] Available at: <http://www.hse.gov.uk/pubns/indg163.pdf> [Accessed 15 July 2014].

Huang, S., Chang, I., Li, S. and Lin, M, (2004). Assessing Risk in ERP Projects: Identify and Prioritize the Factors. *Industrial Management and Data Systems*, 104 (8), p.681 – 688.

Hughes, B. and Cotterell, M, (2002). *Software Project Management*, 3rd edition. London: McGraw-Hill Companies.

Hughes, C, (2009). Managing Enterprise Risk. *Mortgage Banking,* 69(8), p.84-85.

Ikram, N, (2000). *The Management of Risk in Information Systems Development*. Phd Thesis. University of Salford, Salford. UK.

Institute of Risk Management, (2002). *A Risk Management Standard*. [online] Available at: <https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf>[Accessed 25 November 2014].

Institution of Engineering and Technology, (2012). *Quantified Risk Assessment. Techniques - Part 2. Event Tree Analysis - ETA*. Briefing. Health & Safety Briefing No. 26b. [online] Available at: <www.theiet.org/factfiles/health/hsb26b-page.cfm?type=pdf> [Accessed 25 November 2014].

Irwin, A, (1995). *Citizen Science: A Study of People, Expertise and Sustainable Development*. London: Routledge.

ISACA, (2009). *An Introduction to the Business Model for Information Security.* [online] Available at: <http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf> [Accessed 25 November 2014].
ISDR, (2006). *Prevention and Risk Awareness*. [online] Available at: <http://www.eird.org/eng/revista/No10_2005/art21.htm>[Accessed 25 November 2014].

Iskanius, P, (2010). Risk Management of ERP Projects in Manufacturing SMEs. *Information Resource Management Journal,* 23(3), p. 60-75.

Jain, A. and Kalyanam, S, (2012). *Using Insurance to Mitigate Cybercrime Risk*. CapGemini. [online] Available at: <http://www.de.capgemini.com/resource-file-

access/resource/pdf/Using_Insurance_to_Mitigate_Cybercrime_Risk.pdf> [Accessed 25 November 2014].

Jaura, S. and Allan, G, (2005). *An Overview of Project Management*. Portsmouth: University of Portsmouth.

Johnson, E. J, and Tversky, A. (1983). Affect, Generalization, and the Perception of Risk. *Journal of Personality and Social Psychology*, 45 (1), p.20-31.

Jourdan, Z., Rainer, K. R., Marshall, T, E. and Ford, N. F, (2010). An Investigation of Organisation Information Security Risk Analysis. *Journal of Service Science*, 3(2), p.33-42.

Kahneman, D. and Frederick, S, (2002). Representativeness revisited: Attribute Substitution in Intuitive Judgment. In: T. Gilovich, D. Griffin, and D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment*. cambridge: Cambridge University Press.

Kahneman, D. and Tversky, A, (2000). *Choices, Values and Frames*. Cambridge: Cambridge University Press.

Kalinich, K.P, (2013). *Network security and privacy: Risk management and insurance to address legal exposures and financial statement protection. 2013 Update*. [online] Available at: <http://www.aon.com/attachments/risk-services/cyber/Privacy-Update-Cyber-White-Paper-2013.pdf> [Accessed 15 June 2014].

Kaplan, B. and Duchon, D, (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly*, 12(4), p. 571-586.

Karyda, M., Kokolakis, S. and Kiountouzis, E. (2004). Information Systems Security and the Structuring of Organizations. *Proceedings of the 7th International Conference on the Social and Ethical Impacts of Information and Communication Technologies* (ETHICOMP 2004), Syros, Greece, pp. 451-61.

Kaspersky, (2013). *Global Corporate IT Security Risks: 2013*. [online] Available at: <http://media.kaspersky.com/en/businesssecurity/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf>[Accessed 25 November 2014].

Kerzner, H.R, (2009). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*. London: John Wiley & Sons.

King Report, (2009). *King Committee on Corporate Governance: Draft code of Governance Principles for South Africa*. Institute of Directors: South Africa. [online] Available at: <http://www.ecgi.org/codes/documents/king3.pdf>[Accessed 25 November 2014].

Kline, M, (1990). *Mathematical Thought from Ancient to Modern Times*. Oxford: Oxford University Press.

Koller, G, (2005). *Risk Assessment and Decision Making in Business and Industry: A Practical Guide*, 2nd Edition. London: CRC Press.

KPMG, (2011). *The Convergence Evolution: Global survey into the integration of governance, risk and compliance*. [online] Available at: <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/the-convergence-evolutionv2.pdf>[Accessed 25 November 2014].

Kruger, D. J, (2003). Integrating Quantitative and Qualitative Methods in Community Research. *The Community Psychologist*, 36, p.18-19.

Kumar, R. L, (2002). Managing Risks in IT Projects: An Options Perspective. *Information and Management*, 40, p. 63 – 74.

Kunda, Z, (1999). *Social Cognition: Making Sense of People*. Cambridge, Massachusetts: The MIT Press.

Kutsch, E, (2005). *The Effect of Risk Mediators on Project Risk Management and the Project Outcome of Information Technology Projects.* PhD Thesis. University of Bath, UK.

Lapsley, I, (2009). New Public Management: The Cruellest Invention of the Human Spirit? *Abacus,* 45(1), p. 1–21.

Latour, B. and Woolgar, S. (1986). *Laboratory Life: The Social Construction of Scientific Facts*. Princeton University Press, Princeton, NJ.

Lee, W, (2009). *The Influence of Emotion on the Risk Perception and Situation Awareness of Clinicians.* PhD Thesis.

Lerner, J. S., Gonzalez, R. M., Small, D. A. and Fischhoff, B. (2003). Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment. *Psychological Science*, 14 (2), p. 144-150.

Levin, I. P., Schneider, S.L. and Gaeth, G. J, (1998). All Frames are Not Created Equal: A Typology and Critical Analysis of Framing Effects. *Organizational Behavior and Human Decision Processes*, 76, p. 149-188.

Lightle, S. and Sprohge, H, (1992). Strategic Information System Risk. *Internal Auditing*, pp. 6-31.

Lindstrom, J. and Hagerfors, A, (2009). A Model for Explaining Strategic IT and Information Security to Senior Management. *International Journal of Public Information Systems*, 1, p.13.

Linstone, H. A. and Turoff, M, (2002). *The Delphi Method: Techniques and Applications*. Reading, MA: Addison-Wesley Publishing Company.

Loch, K. D., Carr, H. H. and Warkentin, M. E, (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, 17 (2), p. 173-186.

Lopes, L. L, (1987). Between Hope and Fear: The Psychology of Risk. *Advances in Experimental and Social Psychology*, 20, p. 255-295.

Machina, M. and Viscusi, W.K, (2013). *Handbook of the Economics of Risk and Uncertainty.* Oxford: North Holland.

Madu, C., Chu-Hua, K., Madu, A, (1991). Setting Priorities for the IT Industry in Taiwan - A Delphi Study. *Long Range Planning*, 24 (5), p.105-118.

Makowski, M, (2004). *Mathematical Modeling for Coping with Uncertainty and Risk*. [online] Available at: <http://www.iiasa.ac.at/~marek/ftppub/MM/ssr04.pdf>[Accessed 25 November 2014].

Malhotra, N.K. and Birks, D.F, (2007). *Marketing Research: An Applied Approach*, 3rd edition. London:Pearson Education.

March, J. G, (1991). Exploration and Exploitation in Organizational Learning. *Organization Science*, 2(1), p. 71–87.

Mark, C. and Checkland, P, (2003). Soft Systems: A Fresh Perspective for Project Management. In: *Proceedings of the ICE - Civil Engineering*, 156(4), p. 187-192.

Markova, I, (1987). *Human Awareness.* London: Input Brendon Ltd.

Marris, C., Langford, I.H. and O'Riordan, T, (1998). A Quantitative Test of the Cultural Theory of Risk Perception: Comparison with the Psychometric Paradigm. *Risk Analysis*, 18, p. 635-647.

Masing, E, (2009). Technical Support: Improving Performance and Reducing Costs with IT Risk Management. *Risk Management*, 56 (8), p. 48-51.

Matwyshyn, A, (2009). CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices. *Journal of Business Ethics*, 88, p.579 - 594.

McElroy, T., Seta, J. and Warring, D, (2007). Reflections of the Self: How Self-Esteem Determines Decision Framing and Increases Risk Taking. *Journal of Behavioral Decision Making*, 20, p. 223–240.

McLean, K, (1992). Information Security Awareness – Selling the Cause. *In the Proceedings of the IFIP TC11/Sec'92*, 27-29 May, Singapore.

Mehr, R. and Hedges, B, (1963). *Risk Management in the Business Enterprise*. London: Irwin.

Mercantini, J. and Faucher, C, (2015). *Risk and Cognition*. New York: Springer.

Meyers, G, (2006). *Understanding Empiricism*. McGill-Queen's University Press.

Mikes, A., Hall, M. and Millo, Y, (2013). How experts gain influence. *Harvard Business Review,* 91(7-8), p. 70–74.

Mitnick, K, (2003). Best Practice: Are You the Weak Link? *Harvard Business Review*, 81, p.18 - 20.

Mitroff, I.I. and Turoff,N, (2002). Philosophical and Methodological Foundations of Delphi. In: H.A. Linstone, and M. Turoff, eds (2002). *The Delphi method: Techniques and Applications* (pp. 3-12). Reading, MA: Addison-Wesley Publishing Company.

Moore, J. W, (2010). From Phishing To Advanced Persistent Threats: The Application of Cybercrime Risk to the Enterprise Risk Management Model. *Review of Business Information Systems*, 14 (4).

Morgan, M. G. and Henrion, M, (1990). *Uncertainty: A Guide To Dealing With University In Quantitative Risk And Policy Analysis.* Cambridge University Press, Cambridge, UK.

Mumford, E, (1996). *Systems Design: Ethical Tools for Ethical Change*. London: Macmillan.

Murrary-Webster, R. and Pellegrinelli, S, (2010). Risk Management Reconceived: Reconciling Economic Rationality With Behavioural Tendencies. *Journal of Project, Program & Portfolio Management* 1 (1), p. 1-16.

Naderpour, M., Lu, J. and Zhang, G, (2014). A Situation Risk Awareness Approach for Process Systems Safety. *Safety Science,* 64, p.173–189.

National Computing Centre, (2005). *IT Governance: Developing A Successful Governance Strategy: A Best Practice Guide For Decision Makers In IT*. [online] Available at: **<**https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf>[Accessed 25 November 2014].

Neuman, W. L, (2006), *Social Research Methods*. Boston: Pearson Education.

New York Times, (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times*, [online] Available at: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_moc.semityn.www&_r=0> [Accessed 15 July 2014].

NIST, (2002). Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology*, *Special Publication 800-30*: pp. 1-55. [online] Available at: [online] Available at: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30> [Accessed 15 July 2014].

O'Neill, B. and Williams, A, (1998). Risk Homeostasis Hypothesis: A Rebuttal. *Injury Prevention*, (4), p.92–93.

Okoli, C. and Pawlowski, S. D, (2004). The Delphi Method As A Research Tool: An Example, Design Considerations And Applications. *Information and Management,* 41(1), p. 15-29.

Oltedal, S., Moen, B., Klempe, H. and Rundmo, T., (2004). Explaining Risk Perception. An Evaluation Of Cultural Theory. [online] Available at: <http://www.svt.ntnu.no/psy/Torbjorn.Rundmo/Cultural_theory.pdf> [Accessed 15 July 2014].

Ostrom, L.T. and Wilhelmsen, C.A, (2012). *Risk Assessment: Tools, Techniques, and Their Applications*. London: John Wiley & Sons.

Oxford Dictionary,(2013). *Awareness.* [online] Available at: <http://oxforddictionaries.com/definition/english/awareness.> [Accessed 5 February 2013]

Parker Donn, B, (2007). Risks of Risk-Based Security. *Commun ACM*, 50(3), p. 120.

Patton, M. Q, (1987). *How to Use Qualitative Methods in Evaluation*. London: Sage.

Peltzman, S, (1975). The Effects of Automobile Safety Regulation. *Journal of Political Economy*, 83, p.4.

Pember, M. E, (1996). Information Disaster Planning: An Integral Component Of Corporate Risk Management. *Information Management Journal*, 30 (2), p. 31-37.

Pironti, J. P, (2012). *Key Elements of an Information Risk Management Program: Transforming Information Security into Information Risk Management*. ISACA. <www.isaca.org/Journal/Past-Issues/2008/Volume-2/Pages/Key-Elements-of-an-Information-Risk-Management-Program-Transforming-Information-Security-Into-Inform1.aspx>

Poepjes, R. and Lane, M, (2012). An Information Security Awareness Capability Model (ISACM). *Proceedings of the 10th Australian Information Security Management Conference*, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012.

Pohlman, M. B, (2008). *Oracle Identity Management Governance, Risk and Compliance Architecture*, 3rd Edition. New York: Taylor & Francis Group, LLC.

Ponemon Institute, (2011). *2010 Annual Study: Global Cost of a Data Breach*. [online] Available at: <http://www.symantec.com/content/en/us/about/media/pdfs/symantec_cost_of_data_breach_global_2010.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jun_worldwide_idod_codb_9jun> [Accessed 15 June 2014].

Power, M., Ashby, S. and Palermo, T, (2013). *Risk Culture in Financial Organisations*. Research Report for London School of Economics, Centre for the Analysis of Risk and Regulation.

PriceWaterhouseCoopers, (2011). Information Security Breaches Survey 2010 Technical Report. <http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf.>
Prince2.com, (2012). What is Prince2? [online] Available at: <http://www.prince2.com/what-is-prince2-new.asp.> [Accessed 15 July 2014].

Rainer, R.K., Snyder, C.A. and Carr, H.H, (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems,* 8(1), pp. 47-129.

Rashid, S. and Allan, G, (2005). *What Is Effective Risk Management?* Portsmouth: University of Portsmouth.

Razali, A.R. and Tahir, I.M, (2011). Review of the Literature on Enterprise Risk Management. *Business Management Dynamics*, 1(5), p.8-16.

RCUK, (2012). *Research Impact*. [online] Available at: <http://www.rcuk.ac.uk/pages/home.aspx.> [Accessed 15 July 2014].

Rees, J. and Allen, J, (2008). The State of Risk Assessment Practices in Information Security: An Exploratory Investigation. *J Organ Comput Electron Commer*, 18(4), p.255 - 77.

Remenyi, D, (1998). *Doing Research in Business and Management: An Introduction to Process and Method*. London: Sage.

Reuvid, J, (2014). *Managing Business Risk: A Practical Guide to Protecting Your Business London:* Kogan Page Publishers.

Rhee, H-S., Ryu, Y-U. and Kim, C-T, (2012). Unrealistic Optimism on Information Security Management. *Computer and Security,* 31, p. 221-232.

Riley, J, (2004). Compliance Projects Take 40% of Barclay Bank's IT Budget Says Technology Chief. *Computer Weekly*, [online] Available at: <http://www.computerweekly.com/feature/Compliance-projects-take-40-of-Barclays-Banks-IT-budget-says-technology-chief>[Accessed 15 July 2014].

Ritchie, B.W., Burns, P. and Palmer, C, (2005). *Tourism Research Methods: Integrating Theory with Practice*. London: CABI.

Robertson, L.S, (1984). Automobile Safety Regulation: Rebuttal and New Data. *American Journal of Public Health*, 74, p.1390–4.

Robertson, L.S. and Pless, B, (2002). For and Against: Does Risk Homeostasis Theory Have Implications for Road Safety. *British Medical Journal*, 324, p.1149-1152.

Romesburg, C, H, (1984). *Cluster Analysis for Researchers*. California: Wadsworth Inc.

Rottenstreich, Y. and Hsee, C. K. (2001). Money, Kisses, and Electric Shocks: On the Affective Psychology of Probability Weighting. *Psychological Science*, 12, p. 185-190.

Rundmo, T. and Hale, A.R, (2003). Managers' Attitudes Towards Safety and Accident Prevention. *Safety Science,* 41, p.557-574.

Rush, M. and Vednere, G, (1998). Calming the Data Storm: A Risk Management Model For Mitigating Risks. *Information Management Journal*, 42 (4), p. 48-54.

Saunders, M., Lewis, P. and Thornhill, A, (2009). *Research Methods for Business Students*, 5th edition. Harlow: Pearson Education.

Schein, E, (1984). Coming to a New Awareness of Organisational Culture. *Sloan Management Review*, 25(2), p.3.

Schmidt, R., Lyytinen, K., Keil, M. and Cule, P, (2001), Identifying Software Project Risks: An International Delphi Study, *Journal of Management Information Systems*, 17 (4), p. 5 – 36.

Schmittling, R, (2010). Performing a Security Risk Assessment. *ISACA*, 1(1), p.7.

Schneier, B, (2008). *The Psychology of Security*. AfricaCrypt 2008, LNCS 5023, p. 50–79. [online] Available at: <https://www.schneier.com/paper-psychology-of-security.pdf> [Accessed 15 July 2014].

Schwarzer, R, (1994). Optimism, Vulnerability, and Self-Beliefs as Health-Related Cognitions: A Systematic Overview. *Psychology and Health*, 9, p.161 - 80.

Shedden, P., Ruighaver, A.B. and Atif, A, (2010). Risk Management Standards: The Perception of Ease of Use. *Journal of Information System Security*, 6(3), p.23 - 41.

Shostack, A. and Stewart, A, (2008). *The New School of Information Security*. Boston: Addison-Wesley.

Simon, P., Hillson, D. and Newland, K, (1997). *Project Risk Analysis and Management Guide*. London: APM Group Ltd.

Singh, V.P., Jain, S.K. and Tyagi, A, (2007). *Risk and Reliability Analysis: A Handbook for Civil and Environmental Engineers*. London: ASCE Publications.

Siponen, M. T, (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management and Computer Security,* 8, p.31 - 41.

Sjöberg, L. (1997). Explaining Risk Perception: an Empirical Evaluation Of Cultural Theory. *Risk Decision and Policy*, 2(2), p. 113-130.

Sjöberg, L, (1996). A Discussion of the Limitations of the Psychometric and Cultural Theory Approaches to Risk Perception. *Radiation Protection Dosimetry*, 68.

Slovic, P., Finucane, M., Peters, E. and MacGregor, D. (2002). The Affect Heuristic. In: T. Gilovich, D. Griffin, and D. Kahneman Eds. (2002). *Intuitive judgment: Heuristics and biases* (pp. 397-420). New York, NY: Cambridge University Press.

Slovic, P, (2010). *The Feeling of Risk: New Perspectives on Risk Perception*. UK: Earthscan.

Slovic, P., & Peters, E. (2006). Risk Perception and Affect. *Current Directions in Psychological Science*, 15(6), p.322-325.

Speed, T, (2011). *Asset Protection through Security Awareness*. Boca Raton: Auerbach Publications.

Standard and Poor, (2005). *Enterprise Risk Management for Financial Institutions: Rating Criteria And Best Practices*. New York: S & P Publications.

Stanton, N. A., Chambers, P.R.G. and Piggott, J, (2001) Situational Awareness and Safety. *Safety Science*, 39, p. 189-204.

Stoneburner, G, Goguen, A. and Fernga, A, (2010). *Risk Management Guide for Information Technology Systems*. Recommendation of the National Institute of Standards and Technology. Special Publication 800-30. Technology Administration, U.S. Department of Commerce.

Stoney, C, (2007). *Risk management: A Guide to Its Relevance and Application in Quality Management and Enhancement*. Leeds Metropolitan University:

Straub, D. W, (1990). Effective IS Security: An Empirical Study. *Information System Research* 1(2), p. 255-77.

Straub, D. W. and Welke, R.J, (1998). Coping With Systems Risk: Security Planning Models For Management Decision Making. *MIS Quarterly*, .22(4), p.441–469.
Straub, D.W, and Nance, W.D, (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly*, 14(1), p. 45-60.

Tansey, J. and O'Riordan, T, (1999). Cultural theory and risk: a review. *Health Risk Society*, 1(1).

Tarantino, A, (2008). *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental and International Guidance Best Practices*. New York: John Wiley & Sons.

Taylor, C, (2007). Incentives, Behaviour and Operational Risk Management in IT. *The RMA Journal*, 90 (4), p. 50 – 55.

Taylor, R. M, (1990). Situation Awareness Rating Technique (SART): The Development of a Tool for Aircrew Systems Design. In: *Situational Awareness in Aerospace Operations* (Chapter 3). France: Neuilly- sur-Seine, NATO-AGARD-CP-478.

Tesch, D., Kloppenborg, T. J. and Frolick, M. N, (2007). IT Project Risk Factors: The Project Management Professional Perspective. *Journal of Computer Information Systems*, p, 61 – 69.

Tesch, D.B., Kloppenborg, T. J. and Stemmer, J.K, (2003). Investigation of ISAT Research for Project Management Learning. *Project Management Journal*, 34 (4), p. 33 – 39.

Thamhain, H.J, (2014). *Managing Technology-Based Projects: Tools, Techniques, People and Business Processes.* Hoboken: John Wiley & Sons.

Thanopoulos, J, (2014). *Global Business and Corporate* Governance. New York: Business Expert Press.

The Guardian, (2015). *Wikileaks.* [online] Available at: <http://www.theguardian.com/media/wikileaks> [Accessed 15 July 2014].

Tomalin, B. and Stempleski, S, (1993). *Cultural Awareness*. Oxford: Oxford University Press.

Toyoda, H., Kawahashi, I. and Kentaro, N, (2007). Scaling Risk-Taking Tendencies Using Item Response Theory in the Context of Prospect Theory. *Japanese Journal of Educational Psychology*, 55(2), p. 161-169.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E, (2006). Formulating Information Systems Risk Management Strategies Through Cultural Theory. *Information Management & Computer Security*, 14(3), p. 198 – 217.

Urciuoli, V. and Crenca, G, (1989). *Risk Management: Strategie E Processi Decisionali Nella Gestione Dei Rischi Puri D'impresa*. ISBA, Rovereto.

Utin, D.M., Utin M. A. and Utin, J, (2008). General Misconceptions About Information Security Lead To An Insecure World. *Inf Secur J A Glob Perspect,* 17(4), p.164 -9.

van Knippenberg, D, (2011). Advancing Theory in Organisational Psychology. *Organisational Psychology Review*, 1(1), p.3-8.

Vasarhelyi, M, (2002). *Electronic Commerce Security, Risk Management, and Control*. USA: McGraw-Hill.

Venkatesh, V, (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information systems Research*, 11, p. 342–365.

Venkatesh, V. and Bala, H, (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences,* 39(2), p. 273–315.

Venkatesh, V. and Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science,* 46(2), p. 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D, (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* 27(3), p. 425–478.

Verbano, C. and Venturini, K, (2013). Managing Risks in SMEs: A Literature Review and Research Agenda. *Journal of Technology and Managing Innovation*, 8(3).

Vitale, M.R, (1986). The Growing Risks of Information Systems Success. *MIS Quarterly,* 10(4), p.34-327.

Vose, D, (2008). *Risk Analysis*. Chichester: John Wiley and sons.

Walker, P. L., Shenkir, W. G. and Barton, T. L, (2003). ERM in Practice. *The Internal Auditor*, 60(4), p. 51-54.

Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G, (2014). A Situation Awareness Model for Information Security Risk Management. *Computer and Security*, 44, p.1-15.

Weinstein, N.D and Klein, W.M, (1996). Unrealistic Optimism: Present and Future. *Journal of Social and Clinical Psychology,* 15, p.1 – 8.

Whetten, D. A, (1989). What Constitutes a Theoretical Contribution? *Academy of Management Review*, 14 (4), p. 490 – 495.

Wiant, T. L, (2003). *Policy and Its Impact on Medical Record Security*. PhD Thesis. University of Kentucky, Lexington.

Wildavsky, A. and Dake, K, (1990). Theories of Risk Perception: Who Fears What and Why? *Daedalus,* 119, p.41-60.

Wilde, G, (1994). *Target Risk: Dealing with the Danger of Death, Disease and Damage in Everyday Decisions*. London: PDE Publications.

Wilkinson, I, (2001). Social Theories of Risk Perception: At Once Indispensable and Insufficient. In: *Current Sociology*, 49(1), p.1-22.

Wimmer, R.D, (2012). *Mass Media Research*, 10th edition. USA: Cengage Learning.

Wynne, B, (1989). Frameworks of Rationality in Risk Management: Towards the Testing of Naive Sociology. In: J Brown, ed., (1989). *Environmental Threats: Perceptions, Analysis and Management*. London: Belhaven Press.

Yousuf, M.I, (2007). Using Experts' Opinions Through Delphi Technique. *Practical Assessment, Research and Evaluation*, 12(4).

Zachariadis, M., Scott, S. and Barrett, M, (2010). *Exploring Critical Realism as the Theoretical Foundation of Mixed-Method Research: Evidence from the Economics of IS Innovations*. Working paper. Cambridge Judge Business School, University of Cambridge.

Zachmann, K, (2014). Risk in Historical Perspective: Concepts, Contexts, and Conjunctions. In: C. Klüppelberg, D. Straub, and I.M. Welpe, (2014). *Risk - A Multidisciplinary Introduction*, pp 3-35. London: SpringerLink.

Zinn, J. O, (2004). *Literature Review: Sociology and Risk*. Working Paper 2004/1.

Appendices

Appendix A Research Proposal Methodology

The aim of this research is to develop new conceptualisation of a six-element IT risk awareness model and to derive a mathematical model to measure IT risk awareness. The new measure can be used to predict and diagnose risk awareness. It will improve implementation of the assessment and management of risk to Information technology (IT) systems and data in UAE Police Force IT Departments. This will be done through examining practices and levels of risk awareness and professional awareness amongst IT personnel within UAE police forces.

The Risk Management Guide for Information Technology Systems states that "Risk is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability and the resulting impact of that adverse event on the organisation" (NIST, 2002). Moreover, information technology for risk management acquires stores and processes data in electronic format. The potential vulnerabilities or challenges in IT are data loss, media damage, stolen data and inaccessibility of information & data (Data, 2006).

The above general definition of risk does not recognise the importance of the personnel (management and staff) within the process; neither does it recognise the unique requirements of police forces and information technology systems and administration. Bowen (2006) has suggested that the 'human' factor is critical. It is people who are the most vulnerable part of any plan or effort to minimize the risk potential from IT in an organisation. This has been highlighted by audit reports, periodicals and conference etc. (Epich and Persson, 1994; Bowen, 2006). One example to illustrate the human influence on risk management is the following: If one employee damaged a storage device and there is no backup for the data this will result in data loss. To handle such challenges effectively, an integrated risk management approach is required. As identified by number of researchers (Rainer et al., 1991; Eloffr et al., 1993; Epich and Persson, 1994; Lightle and Sprohge, 1992; Lochr et al., 1992; and Vitale, 1986), there are three major risk management components namely; risk identification, risk analysis and risk-reducing measures should be taken into consideration to prevent such risk.

Risk awareness is regarded as new concept to be introduced in this research and particularly important to the police force. Police Forces' IT consist of Finger Print, Iris, Crime Data and information about their employees and finance. To enter or retrieve the information electronically, every officer within the police force becomes part of the IT system. Therefore,

they need to be aware of risk. For example, this awareness led to a major decision in UAE Police Force. In 2008, Abu Dhabi Police was operating on one database server. A decision was made by the authorities to have a contingency plan, which was to have another database server clone to the main database but placed in another city almost 100Km away and networked directly with the main server. The aim is to avoid loss of data in non-desirable threat events in the future. Though this action is required but it dealt with the problem at hardware level and did not include the staff factor. Hence, it is essential that staff should be aware of the immediate intention and action to substitute their database with the main one.
The literature review carried out here shows that there are only three projects suitable to MERIT. These three projects listed below span between 2000 and 2008. For the last 3 years there is no relevant project in line with MERIT.

Ikram (2000) carried out an empirical study into the management of risk information systems, the nature of risks, current risk management practices and their effect on IS development in the UK. Ikram (2000) observed that there has been a lack of rigorous research into risk management, particularly on the human factor. Ikram (2000) defined three parameters that poses the most serious risk issues in information systems; Estimation, Organisation and Personnel Capabilities. Ikram developed an appreciative model of risk management that offers a basis for carrying out new research tasks. Ikram's research utilised the model to describe and analyse risk management process in IS development. However, the model was not tested in a practical implementation as the aim was to develop a theoretical model only. Therefore, Ikram's study did not include an observation of the human factors within the process of risk management.

Al-Fehaid (2003) investigated risk in IT Accounting Audit. The aim was to expand this theoretical model and apply it to Risk Assessment. Al-Fehaid has reported that one of the limitations of his work is the scope of applying the developed theoretical model to other countries as it is limited to only KSA. Al-Fehaids' model has articulated set of variables that have sprung up from KSA and hence this limitation.
A third study that forms the present work by Kutsch (2005) investigates how interventions influence risk management and ultimately improves the ability to prevent risks from adversely altering the outcome of IT projects. Kutsch (2005) argued that the lack of awareness of risks by IT project managers would have an adverse influence on the outcome of IT projects. Kutsch has suggested that in order to prevent risks from adversely influencing

the project outcome, IT projects managers should plan early to prevent risk related interventions from influencing the use of project risk management

In conclusion, survey of data risk management within the last decade suggests that risk awareness is not understood or addressed by most organizations (Gartner, 2012). This study builds on the work of Kutsch (2005) and others and aims to generalise the importance of awareness amongst **all** staff within an organisation with particular theoretical focus on the requirements of police force IT departments.

This research will examine six parameters that could contribute to risk management and referred to in this research as risk processes. Tarantino (2008) lists three elements as Governance, Compliance, and Risk Management in none specific order. Pohlman (2008) lists five elements as Governance, Compliance, and Risk Management**,** Enterprise and IT GRC in none specific order. The elements of these processes including Risk Awareness element are depicted in Figure 1. These elements listed and linked to reach risk awareness. This model is new to knowledge and it will be the route to develop a novel mathematical approach which may be applied to the UAE Police force and tested against simulation software such as ArcSight or Wolfram Mathematica. The results of the new mathematical model will be verified and evaluated.

Figure 1: The Elements Composing Staffs' Risk Awareness

The argument and logic underpinning Figure 1 is based on human or staffs' awareness of risk, whereas previous studies have identified these elements (Tarantino, 2008; Pohlman, 2008), they have not focused on the people aspect of risk management and in particular staffs' risk awareness. This is a new perspective of this research. The order of the elements in the Figure 1 pyramid is significant because the unit of analysis is people or staff. Staff should be aware of the governance policies of the organisation which is the bottom level. They are then required to comply with the policies, which is the second level of compliance to the requirements of risk management. Staff should be familiar with organisation or enterprise processes, which is the third level. For IT staff, these three levels, governance, compliance and enterprise, form the IT GRC forth level of the pyramid. This then enables them to understand risk management which is the fifth element. When staff understand and comply with all these five elements, then they can be said to be risk aware, the final top level of the pyramid.

Figure 1 shows six elements that are currently in practice in the industry. The definitions of these elements are listed below:

Governance:

Governance is the system by which organisations are directed and controlled. Within a department it is the policies and procedures used for IT risk management. Governance is the system by which the Abu Dhabi Police Force is directed and controlled and is used to manage its resources, including financial, human resources and information resources. This research seeks an appropriate governance model for Police Force in UAE to manage IT risks.

Compliance:

Good compliance within an organisation mandates that employees need to observe the requirements of government systems and adhere to the policies in order to reduce any risk. It requires a good level of knowledge i employees achieved through training.

Enterprise is a project or a mission through which the organisation delivers products or services. Enterprise is a business organisation, an organisation created for business ventures. In other words, an enterprise is a project or a mission that produces products and services. The UAE Police Force is one such enterprise.

IT GRC refers to a unified, comprehensive and inter-connected approach towards Governance, Risk Management and Compliance that relates to the organization's use of Information Technology (IT). IT GRC (Governance, Risk Management and Compliance) is

new directive to industry management. However, it compels industry to make use of IT to present a unified, comprehensive, and inter-connected approach towards a successful organisation. The major factor within this element is using the skill and adventure of IT to its maximum advantage and latest developments.

Risk Management is an overarching organisational framework intended to protect an establishment from the negative impact of risky incidents which are encountered in their normal course of business. Is an overarching organisational framework intended to protect an establishment from the negative impact of risky incidents which are encountered in their normal course of business. Risk management is a method used to reduce a risk which is unexpected in organization and it contains the main elements or processes risk identification, risk assessment, and risk control. **Risk management seeks to manage risk around the key products and services that an organisation delivers.** Risk *management* is the process of analyzing the risks faced by an undertaking and putting in place the organizational capabilities required to respond appropriately should any of those risks occur.

MERIT Risk Awareness is newly proposed intended to facilitate our understanding of staff responses to manifestation of negative incidences through the reliance of practical knowledge awareness and professionalization of all staff members. Since awareness is a human quality, this element focuses on measuring the effect of the previous elements on managers and staff level of awareness of risk.

Governance, compliance, enterprise, IT GRC and risk management should result in managers and staff risk awareness. These elements of the conceptual model will be explored by (a) scoping their presence in UAE enterprises, phase one of the research methodology, using ten enterprises ranging from small, medium to large enterprises to respond to 119 questions covering the above elements and comprising descriptive and analytical research; (b) developing mathematical models of risk awareness and management, phase two of the research methodology, comprising deductive mathematical and predictive research; and (c) applying the mathematical model to the UAE police force, phase three of the research methodology using the Delphi method.

Methodology

To achieve professionalism within the Police Force's IT department in the UAE, the work will be undertaken in three stage processes:

1. Scoping: IT risk awareness and management: (meets objectives 1 and 2)

a. To determine the various critical facets of employee risk awareness, IT risk management practiced in small, medium, large and corporate organisations that can be applied to police forces. This will be done by formulating a questionnaire to collect descriptive categories of data from the UAE Police Force IT Department.
b. Through a questionnaire, a survey of a range of small, medium and large business organisations will be carried out to determine the best practice in successful employee risk awareness and IT risk management. The questionnaire comprises 119 questions which represent the defined parameters and criteria for modelling and evaluating IT risk awareness management.
c. Assess employee risk awareness and professional responsibility to inform IT risk management in police forces in the UAE. This will be done through the descriptive categories collected from 1. (a) and statistical categories collected from 1. (b).

2. Modelling: IT risk awareness/management modelling and development: (meets objective 4)
    a. Evaluate and model levels of IT risk awareness to verify and evaluate the new mathematical model developed by this research project. This will be done by taking the outcomes of the scooping (1.a and 1.b) as inputs to invent the mathematical models and using the Delphi method of expert knowledge.
    b. Evaluate and model levels of responsibility for IT risk management amongst employees and how management is delegated among employees of the police forces. This will be done using the Delphi method of expert knowledge.
    c. Critically evaluate methods of dissemination and training of IT risk awareness, professionalism and management issues to employees within police departments. The new model categories will identify specific duties that usually exist but are overlapped between managers and staff. A novel mathematical model, based on the conceptual model, will be developed to formalise the risk management processes. Hence, this research will be able to improve quality and success of risk management through predictive and diagnostic metrics.

3. Development/evaluation: IT risk awareness/management training for police forces: (meets objectives 3)

a. Using the Delphi Method refine new model which links risk awareness to behavioural and managerial indicators of professionalism and successful risk management operation assessed against defined criteria in a security context.
b. Using the Delphi Method develop and evaluate improvements to IT risk management methodologies and training and assessment of professionalism for police forces, incorporating examples of best practice from other organisations such as Banks.
c. Using the Delphi Method finalise a predictive model linking training needs to requirements for professionalism, awareness and management of IT risk.

The criteria for selecting organisations within the methodology of this research project are based on:

1. Profitable or non-profitable
2. Private or Public
3. Small or large

The outcome will include methods for diagnosing current levels of awareness and the training required to successfully implement the information risk management policy. To achieve this, this research will carry out an exploration of current IT risk management practice in the UAE (in comparison to UK) and its effectiveness on the management of IT systems with police forces. The research will be carried out in three stages**:** Scoping of IT risk awareness in management & staff; modelling the critical 'predictive' elements & the relationship between them; Development & implementation of training protocols and their evaluation. The existing knowledge of empirical studies carried out by Ikram (2000), Al-Fehaid (2003) and Kutsch (2005) will be incorporated into a novel mathematical model will make an original contribution to knowledge. This is new knowledge since no other research in IT risk management has developed a novel mathematical approach to modelling the IT risk management environment. The aim of the research outlined here is to represent the different components shown in Figure 1 in a quantifiable model that is both analytical and predictive.

Dealing with Ethical issues

The researcher is a Senior Police Officer in the UAE police force, which may be a cause for concern amongst participants. However, a strict code of conduct would be formulated for gathering information from the participants who will mostly be employees of the UAE. To resolve ethical issues involved in the study, all participants will be volunteers and will be provided with a clause of confidentiality. This would ensure that the identity of the participants is kept confidential. In this regard, a consent agreement to this effect would be

provided to the participants. They would also be informed about how the information provided by them would be used in the study. Only relevant information would be collected and used for the purpose of the research**.**

Research Plan

The following table represents the plan for the remaining period of this research program: (Note due to delays resulting from changes in Faculty and submission/resubmission of RD1, some of this work has already been carried out or is currently underway)

Items	Tasks	Duration
1	Studying the topic	March 2009-August 2009
2	Literature Review	September 2009- December 2009
3	Defining the problem	January 2010-March 2010
4	Survey	March 2010-May 2010
5	Designing a Pilot Study	May 2010-July 2010
6	Pilot Study Data Collection	August 2010-October 2010
7	Pilot Study Data Collation/Analysis	November 2010-January 2011
8	Designing and developing new model to the Risk Awareness	February 2011-June 2011
9	Main Data Collection	July 2011-September 2011
10	Data Analysis	October 2011-December 2011
11	Training Development/Implementation	January 2012 – March 2012
12	Evaluation of Training and outcomes	April 2012- May 2012
13	Refinement of Model and Protocols	June 2012 – July 2012
14	Thesis Write-Up and Submission	August 2012 – January 2013

Appendix B Questionnaire to Assess Current Risk Management

Questionnaire

To understand the current risk management data were collected using a questionnaire. The data were collected from the ITT Department. This was conducted over two weeks in May 2008.

This questionnaire is to collect information that is important to research for the Abu Dhabi Police. Please assist this important work by answering all the questions in your own time.

Section 1: Questionnaire about Risk and Business Continuity Planning (BCP)

Q1. When a problem occurs in your work which of the following events do you think comes first?

a. Crisis b. Risk c. Disaster d. Emergency

Q2. To what extent do the above events effect the continuity of products and services?

a. Highly b. Rarely c. I do not know d. little effect e. No effect

Q3. Do you agree there is risk in every aspect of your work?

a. Strongly agree b. Agree c. Disagree d. Strongly disagree

e. I don't know

Q4. How do you rate your experience with risk?

a. Very experienced b. experienced c. Some experienced

d. little experience e. No experience

Q5. From your experience is there a process that can deal with risk in your work?

a. yes b. Maybe c. I do not think so d. No

Q6. To what extent do you think yourself familiar with Business Continuity Planning?

a. Expert knowledge b. Some knowledge c. Very little knowledge

d. No knowledge e. I don't know

Q7. Do you think Business Continuity Planning will be suitable for your work?

a. Strongly agree b. Agree c. Disagree d. Strongly disagree

e. I don't know

Section 2: Questionnaire for A role of Information Technology & Telecommunication (ITT)

Q8. What is the role played by Information Technology and Telecommunications when crisis occurs?

a. Important role b. Small role c. Minor role d. No role

Q9. All organizations who deal with ITT must have a plan to avoid risk?

a. Strongly agree b. Agree c. Disagree d. Strongly disagree

e. I don't know

Q10. From your point view, do you think there is a relationship between Business Continuity Planning and ITT?

a. Strong relation b. Small link c. little relationship d. No relationship

e. I don't know

Q11. How can we improve this relationship?

a. By build plan b. By build framework c. By build strategic d. All what mention

Q12. Do you think that ITT equipments or tools play an important role during risk, crisis and disaster?

a. Strongly agree b. Agree c. Disagree d. Strongly disagree

e. I don't know

Appendix C Arabic Version of Questionnaire

Appendix F

استبيان

هذا الاستبيان لجمع المعلومات الهامة لبحث يتم تنفيذه لحساب شرطة ابوظبي.
يرجى المساعدة في هذا البحث من خلال الإجابة عن جميع الأسئلة في غير وقت العمل.

القسم الأول: الاستبيان عن تخطيط استمرارية العمل

س١ : عندما تحدث مشكلة في عملك أي من الحوادث التالية باعتقادك تأتي أولا ؟
أ- أزمة ب- مخاطرة ج- كارثة د- طوارئ

س٢- إلى أي مدى تؤثر الحوادث أعلاه على استمرارية المنتجات والخدمات؟
أ- بدرجة عالية ب- نادرا ج- لا أعلم د قليلا هـ لا تؤثر

س٣- هل توافق على ان هناك مخاطرة في كل جانب من جوانب عملك؟
أ- أوافق بشدة ب- أوافق ج- لا أوافق
د- لا أوافق أبدا هـ لا أعلم

س٤- كيف تصنف خبرتك فيما يتعلق بالمخاطر؟
أ- خبير جدا ب- خبير ج- بعض الخبرة
د- قليل من الخبرة هـ لا خبرة البتة.

س٥- من واقع تجربتك الشخصية، هل هناك إجراءات للتعامل مع المخاطر في عملك؟
أ- نعم ب- ربما ج-٠لا أعتقد د- لا

س٦- إلى أي مدى تعتقد نفسك مطلعا على التخطيط لاستمرارية العمل؟
أ- معرفة الخبير ب- بعض المعرفة ج- معرفة ضئيلة
د- لا توجد معرفة هـ لا أعلم

س٧ – هل تعتقد ان التخطيط لاستمرارية العمل مناسب لعملك؟
أ- أوافق بشدة ب- أوافق ج- لا أوافق
د- لا أوافق أبدا هـ لا أعلم

الجزء ٢- استبيان بشأن دور تقنية المعلومات والاتصالات

س٨- ما هو دور تقنية المعلومات والاتصالات في خال وقوع أزمات؟

أ- دور هام ب- دور قليل ج – دور ثانوي د- لا دور لها

س٩- يجب ان تتوفر لدى جميع المؤسسات التي تتعامل مع تقنية المعلومات والاتصالات خطة لتجنب المخاطر

أ- أوافق بشدة ب- أوافق ج- لا أوافق

د- لا أوافق أبدا هـ- لا أعلم

س١٠- هل تعتقد ، من وجهة نظرك الخاصة، ان هناك علاقة بين استمرارية العلم وبين تقنية المعلومات والاتصالات

أ- علاقة قوية ب- ارتباط قليل ج- علاقة ضئيلة د- لا توجد علاقة

س ١١- كيف يمكن لنا ان نحسن هذه العلاقة؟

أ – بوضع خطة ب- بوضع إطار عمل ج- بوضع إستراتيجية د- كل ما ذكر

س ١٢- هل تعتقد ان أجهزة وأدوات تقنية المعلومات تضطلع بدور هام خلال المخاطر والأزمات والكوارث؟

أ- أوافق بشدة ب- أوافق ج- لا أوافق

د- لا أوافق أبدا هـ- لا أعلم

Appendix D Comparative Case Interview Questions

Q1. What is the role played by Information Technology and Telecommunications when risk occurs within your organisation?

Q2. All organisations who deal with ITT must have a plan to avoid risk. Does your organisation have a Risk Management strategy or plan?

Q3. Are people in your organisation aware of risk and how to deal with it?

Q4. From your experience what is the advice that you can give to build a good plan or strategy for Abu Dhabi Police (ITT Department)?

Appendix E Delphi Consensus Method for Conceptual Model

The Delphi method originated at the RAND Corporation in the late 1960's as a forecasting methodology. The U.S. government then enhanced it as a group decision-making tool. The Delphi method is used to achieve the consensus of group of experts on subjective factors. The Delphi method is a structured communication technique and was developed as a systematic, interactive forecasting method using a panel of experts. The principle governing the Delphi method is that forecasts or decisions from a well-defined expert structured group are more valid and defined as 'collective intelligence' (Okoli and Pawlowski, 2004). There are policy-making versions of the method and it has been adapted from face-to-face meetings referred to as mini-Delphi or Estimate-Talk-Estimate (ETE). Delphi is widely used in business forecasting.

The Taiwan government used the Delphi method to prioritize the country's Information Technology industry, Madu et al., (1991) conclude:

"Finally, these decisions reflect the experts' world views, life experiences, cognitive feelings and perceptions. Thus, these results are based on the participants' subjective assessments which may also be influenced by data. Decision-making in itself is subjective. However, the use of experts in a systematic manner will yield a satisfactory solution to sociotechnical problems." (Madu et al., 1991)

Cline (2012) notes the subjective features of the problem which requires formal definition:

"Delphi has the added advantage that it works as an informal, subjective model when the decisions are based on opinion, and can be directly converted to a formal model, when the data is more knowledge-based."

Delphi Consensus Survey

Abu Dhabi Police Force

Khalid Bin Ishaq

Delphi is based on the principle of expert decisions or "collective intelligence". The Delphi method involves members of expert panel individually and separately answering a questionnaire in two or more rounds. After each round, a facilitator will provide anonymous summary of your expert forecasts from the previous round, as well as the reasons they provided for their judgments. As experts you are encouraged to revise your earlier answers in light of the replies of other members of the Delphi panel. It is believed that during this process the range of the answers will decrease and the expert panel will converge towards the "correct" answer. Finally, the process will be stopped after two rounds. The Delphi method will be used for normative and explorative use, to provide guidelines for IT risk management to the Abu Dhabi Police Force.

Example Delphi Method

The Delphi Method will consist of two anonymous rounds. In the first round you, as the anonymous expert, will indicate your scores, as shown in brackets (75). Then a different expert will give their score, shown in square brackets [85] in the light of your score. Finally, you will be given the opportunity to re-consider your score in the light of the other experts' score, which you will enter, shown in cheverons <80>.

1.	On a scale of 0% to 100%, what is your current level of direction and guidance on risk management given to employees?	0% 100% |_____(75)_<80>_[85]___|

Governance Model

Governance is the system by which the Abu Dhabi Police Force is directed and controlled and is used to manage its resources, including financial, human resources and information resources. This research seeks an appropriate governance model for Police Force in UAE to manage IT risks.

Please write the values on the scale.
Example:

0% 100%
|_____25%_____|

1. On a scale of 0% to 100%, what is your current level of direction and guidance on risk management given to employees?

0% 100%
|_____|

2. On a scale of 0% to 100%, what is your current level of feedback given to employees?

0% 100%
|_____|

3. On a scale of 0 days to 90 days, how many days does it take employees to train, familiarize themselves and apply the guidance?

0 days 90 days
|_____|

4. On a scale of 0 (not aware) to 100 (fully aware), what is the current level of risk awareness by governance?

0 100
|_____|

Compliance Model

Good compliance, within an enterprise, mandates that employees need to observe the requirements of governance systems and adhere to the policies in order to reduce any risk. Therefore, the enterprise must follow this strategy by increasing the level of knowledge and skills of employees in accordance with the requirements for compliance.

Compliance is the act or process of the enterprise to comply with regulations imposed by the governance. One of the items that should be complied with is the data. The enterprise has to make sure that staffs are familiar with these regulations and do they apply them to citizens. Enterprise must make sure any stored data are stored securely.

Please write the values on the scale.
Example:

0% 100%
|_____25%_____|

5. On a scale of 0% to 100%, what is your current level of employee understanding of risk management requirements?

0% 100%
|_____|

6. On a scale of 0% to 100%, what is the level of feedback you give to employees?

0% 100%
|_____|

7. On a scale of 0 days to 275 days, what is the number of days training given on compliance to employees?

0 days 275 days
|_____|

8. On a scale of 0 (not aware) to 100 (fully aware), what is the current level of risk awareness of your employees?

0% 100%
|_____|

Enterprise Model

Enterprise is a business enterprise, an enterprise created for business ventures. In other words, an enterprise is a project or a mission that produces products and services. The UAE Police Force is one such enterprise.

Please write the values on the scale.
Example:

0% 100%
|_____25%_____|

8. On a scale of 0% to 100%, what is the level of quality you achieve for the service you provide?

0% 100%
|_____|

9. On a scale of 0% to 100%, what is the level of feedback on quality you get from citizens, governance and employees?

0% 100%
|_____|

10. What is the size of the police force? Please circle one option.

Small medium large

|_____|_____|_____|

33% 66% 100%

IT GRC Model

IT GRC (Governance, Risk Management and Compliance) is new directive to industry management. However, it compels industry to make use of IT to present a unified, comprehensive, and inter-connected approach towards a successful enterprise. The major factor within this element is using the skill and adventure of IT to its maximum advantage and latest developments.

Please write the values on the scale.

Example:

1 12

|_____4_____|

11. On a scale of 1 to 12, how many meetings do you think are necessary to coordinate and unify risk awareness?

1 12

|_____|

12. How many employees does the enterprise employee?

1 n

|_____|

13. What is the level of skills of your IT employees?

1 100

|_____|

Risk Management Model

Is an overarching enterpriseal framework intended to protect an establishment from the negative impact of risky incidents which are encountered in their normal course of business. Risk management is a method used to reduce a risk which is unexpected in organization and it contains the main elements or processes risk identification, risk assessment, and risk control. **Risk management seeks to manage risk around the key products and services that an enterprise delivers.** Risk *management* is the process of analyzing the risks faced by an undertaking and putting in place the organizational capabilities required to respond appropriately should any of those risks occur.

Please write the values on the scale.

Example:

1 100

|_____4_____|

14. On a binary scale of 1 (correctly) or 0 (wrongly), has your enterprise identified risks? Please circle one option.

1 0

|_____|

15. On a scale of 0 (worst) to 100 (excellent), indicate the level of risk assessment achieved by your enterprise.

1 100

|_____|

16. If risk were to occur, what is the magnitude of its impact on the enterprise?

1 100

|_____|

17. What is the potential of the risk occurring?

0 100

|_____|

18. On a scale of 0 (no measures) to 100 (full measures), indicate the level of measures your enterprise has taken to prevent risks.

0 100

|_____|

Appendix F Project Information & Consent

THE PROJECT

&

OUR CONTACT DETAILS

MERIT: the ManagEment of Risk awareness in relation to Information Technology

In order to help you consider whether your involvement in this programme of study will be of relevance to you and your enterprise, it is important to elucidate the underlying motivations of the study and what exactly is involved in this stage of the study. Please spend a little time to understand the contents of this information leaflet which is designed to clarify major questions you may have on the subject. If there is anything unclear, or if you would like further information, please do not hesitate to contact any member of the research team based in the UK who will be delighted to assist you:-

UK Contact Details:-

Att. Lt. Col. Khalid Bin Ishaq, Dr Kevin Hapeshi and Dr David Wakeling
The Business School
Faculty of Computing
University of Gloucestershire
Broadlands Villa, The Park
Cheltenham, **GL50 2RH**

Email: khalidbinishaq@connect.glos.ac.uk
Phone (UK): +44 (0)1242 714 087
Mobile (UK): +44 (0)7880 697 455
(Monday – Friday 10:00 – 16:00)

UAE Contact Details:-

Lt. Col. Khalid Bin Ishaq
P.O. Box 31356 Abu Dhabi
Mobile (UAE): +97 1507 309 339
(Sunday-Thursday 7:30 -14:30)

ABOUT THIS STUDY

What is MERIT?

IT has brought about many excellent advantages to enterprises in a variety of ways, for example, that speed up processes of storage and retrieval of information for efficiently conducting it's business. However, this success has also brought about huge risks, such as data security violation, commercial and financial security, etc., which can seriously undermine the stability of an enterprise, and in severe cases result in serious financial or commercial instability and ruin.

MERIT is a process/algorithm that seeks to minimise the risks to the enterprise by focussing on Risk Awareness issues in order to pre-empt the manifestations of risky incidents.

What is Risk Management?

Risk Management is a methodology which is widely adopted by many enterprises in the quest to minimise, or eliminate, the manifestations of all conceivable risky incidents.

What is Risk Awareness?

Risk Awareness is a self-regulating process, applicable to all members of staff within an enterprise, to facilitate the identification of possible risks faced by the enterprise.

How long will the MERIT study run?

MERIT is a research study programme that spans over a three to four year period.

What is the purpose of MERIT?

In terms of benefits to the enterprise, MERIT seeks to guarantee success and expansion by minimising the impact of identifiable risky incidents on the operational stability of the enterprise.

What type of risk will be considered?

Enterprises are susceptible to a vast plethora of risks that can be categorised under several broad headings, namely, risks relating to health, natural disasters, financial crisis, war & terror and IT related security issues. In this study, we focus primarily on IT, which has been a sector within which very large-scale dependencies in the utilisation and safe guarding of sensitive or valuable data and the associated risks relating data security breach. Such IT related risks poses significant challenges to enterprises of all sizes, irrespective of the nature

of the business (i.e. global, national or local) or whether they are profit- or non-profit making enterprises (c.f. supermarket versus law enforcement department).

Who is conducting this study?

This study is conducted by a research team within The Business School at the University of Gloucestershire, led by *Dr. Kevin Hapeshi*, *Dr David Wakeling* and *Lt. Col. Khalid Bin Ishaq*.

Who is funding this study?

The study is being supported by the office of the Abu Dhabi Police at the UAE Embassy, London, UK.

Why is this research important?

A large number of enterprises are susceptible to catastrophic failures because of inadequate implementation of essential Risk Assessment processes. In part, this is due to lack of appreciation of the importance of Risk Assessment and in part, it is due to lack of concrete evidence to emphasise its importance in a pre-emptive role within the overarching Risk Management framework. This research addresses both these issues, the results of which can help minimise the volatility of enterprises of all sizes (namely, small, medium and large) through the proper and adequate application of Risk Awareness processes.

YOUR ROLE IN THIS PROJECT

How have I been chosen for invitation into MERIT?

Your organisation has been selected to take part in this study because it has vast experience and is well established in its line of business for several years. It is also a well known organisation and based within the UAE; a geographical significant area of interest to our sponsors.

Why should I take part?

You, and your organisation, lie in a group of enterprises that are regarded as being potentially susceptible to destabilising effects stemming from high risk incidents and would benefit considerably from the findings and feedback of this research, based on our analysis of survey data which you will provide.

Do I have to take part in the MERIT study?

Yes! The experience and long establishment of your enterprise is unique and realistic for testing and obtaining the necessary data to validate the MERIT approach to pre-emption through Risk Awareness.

What does taking part in MERIT involve?

Participation involves providing answers to a set of straight forward questions which accompany this information leaflet, and returning it promptly to the address mentioned within the time-frame specified.

Will I benefit if I take part?

Yes! The findings and results of this study will be provided to you, upon request.

INFORMATION REQUIRED

What information is needed for this study?

For this study we need to collect information about six specific areas of your company. These are:

1. **Governance:** This is a fundamental function to any enterprise. It is known that Good Governance involves:

   - Accountability

   The system has to be liable to be called on to render or bear the consequences for failure or success

   - Participation

   All have to be involved or given the option to be involved in setting up governance rules

   - Predictability

   To be prepared for worst case scenario events, predications should be considered

   - Transparency

   No hidden agenda to any member of the organisation

2. **Enterprise Risk Management (ERM): This 2nd element that is defined formally and related to the Governance element.** There are different meanings of ERM but the most appropriate one for this research area is an organisation created for business ventures with the aim of eliminating any risk for itself and other establishments.

3. **Compliance:** Good compliance, within an organization, mandates that employees need to observe the requirements of government systems and adhere to the policies in order to reduce any risk.

4. **IT GRC:** refers to a unified, comprehensive, and inter-connected approach towards Governance, Risk Management and Compliance that relates to the organization's use of Information Technology (IT).

5. **Risk Management:** Risk management is a method used to reduce a risk which is unexpected in organization and it contains the main elements or processes are risk identification, risk assessment, and risk control.

6. **Risk Awareness:** Risk awareness is a combination of vulnerability assessment and knowledge management, which provides critical input to the risk identification and risk management process

The attached questionnaire covers the above six elements at various levels. By answering the associated questions whether by ticking, given brief description or assigning a number, you will be kindly providing us with the required research technical information.

YOUR CONSENT

Why do you need my consent?

We need your consent to comply with Data Protection laws and observe the common law duty of confidentiality owed to participants. This gives the *University* of *Gloucestershire* your permission to hold and use information that may identify you anonymously. It also allows us to send you the research feedback at your request.

How can I withdraw my consent?

You have the right to withdraw at any time. If you are considering withdrawing from the study, please contact the phone number listed in the covering letter.

If you do decide to withdraw, you will have the following options concerning future contact and use of your data:

1. No further contact – this means that this research team would no longer contact you directly, but would still have your permission to retain and use information provided previously and to obtain and use other information from your records.

2. No further access – this means that this research team would no longer contact you or obtain further information from your records in the future, but would still have your permission to use the information provided previously.

3. No further use – this means that, in addition to no longer contacting you or obtain further information, this research team would destroy all of your information previously provided.

YOUR ANONYMITY

&

DATA PROTECTION

How will information about me be kept confidential?

Your privacy and confidentiality are important to us. The *University* **of** *Gloucestershire* has sought advice from the information Commissioner to ensure that this research study complies fully with the requirements of the **Data Protection Act 1998**. All data will be stored securely on a private computer network at the *University* **of** *Gloucestershire.* The results of this study will be published following independent review but no individually-identifying data will ever be published.

Who will be able to access and use my information?

All data will be stored securely on a private computer network at the *University of Gloucestershire* and will be accessed by the academic research team. Your identifying information including name and address will be kept separately from public use. Access to your information will be limited to a few members of the academic research team at All data will be stored securely on a private computer network at the *University* **of** *Gloucestershire* who will be required to sign strict non-disclosure agreements.

THE NEXT STEPS

What should I do if I now want to take part?

If you would like to help by taking part, please complete the attached questionnaire. Please provide your consent. Please insert in and post the answered questionnaire the provided self-stamped envelope.

When do I have to decide?

You have four weeks to think over and complete.

What can I do if I'm unsure about taking part or have any other concerns or queries?

Should you have any concerns or queries we would be pleased to provide you with further information:

1. By writing to the address:

UK:

Khalid Bin Ishaq
The Business School
Faculty of Computing
University of Gloucestershire
Broadlands Villa, The Park
Cheltenham, GL50 2RH

UAE:

P.O. Box 31356 Abu Dhabi
Mobile (UAE): 00971507309339
(Sunday-Thursday 7:30 -14:30)

2. By email: khalidbinishaq@connect.glos.ac.uk

3. By Phone: +44 7880 697 455 (UK)

   +97 1507 309 339 (UAE)

EXAMPLEs ON THE QUESTIONNAIRE

The questionnaire is designed to make answering as easy as possible. Answering mostly involves selecting one or several options (numbers) which represent your answer as accurately as possible as shown in the following illustrations provided below as a guide:-

Example Question 1:

EQ1. Is the sun important for the planet?

Your answer: [0 1 2 3 (4) 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Example Question 2:

EQ2. Are you connected to broadband? *Comment: This question affects question EQ3.*

Your answer: [0 (1) 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Example Question 3:

EQ3. What is the speed of your broadband connection? *Comment: Because A2= No this is not applicable*

Your answer: [0 (1) 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Example Question 4:

EQ4. Do you expect to have broadband within the next 12 months? *Comment:* Can only be 0 or 1 (0)

Your answer: [0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Please answer the following straight-forward questions now. All answers will be treated STRICTLY ANONYMOUSLY:-

THE 6 ESSENTIAL ELEMENTS OF RISK MANAGEMENT

There are 6 elements to answer within this set of questionnaire:

Element 1: GOVERNANCE

What is Governance?

It is the system by which the organisations are directed and controlled.

It has been mentioned in some literature as Good Governance instead of Governance, but both lead to the same aim. Good governance requires that decisions are made and implemented using a clear and legitimate process, to achieve consistent and effective policies. It can be applied at international, national, local, and organizational levels and to manage many types of resources. Good Governance involves:

- Accountability

The system has to be liable to be called on to render or bear the consequences for failure or success

- Participation

All have to be involved or given the option to be involved in setting up governance rules

- Predictability

To be prepared for worst case scenario events, predications should be considered

- Transparency

  No hidden agenda to any member of the organisation

Q1. Does **Governance** mean anything to you?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q2. Is **Governance** transparent to you within your organisation?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q3. Have you contributed to the development of the **Governance** regulations?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q4. How can we improve **Governance**?

_____

_____

_____

How many types of governance models?

There are quite few models but I would like to list the closest one to this research project and mainly related to non-profitable organisations:

Operational Model: The board manages, governs and performs the work of the organization.

Collective Model: The board and staff operate as a single team when making decisions about governance and the work of the organization. Board members may work with either or both service operations or management functions.

Management Model: The board manages operations through functional committees that may or may not have a staff coordinator.

Constituent Representational Model: An approach used by publicly elected officials. Federations or other constituency-elected boards have the primary responsibility of balancing the interests of their constituents with the best interests of the organization.

Traditional Model: The board governs and over-sees operations through committees established along functional lines (finance, human resources, and programs) but delegates the management functions to the executive director.

Results-based Model: The executive director is a non-voting member of the board, carries substantial influence over policy making, and is viewed as a full partner with the board. Committees, organized around board responsibilities and lead planning, would guide

governance, and monitor and audit performance of the board, executive director and organization.

Policy Governance (Carver) Model: The board governs through policies that establish organizational aims (ends), governance approaches, and management limitations. These policies also should define the relationship of the board with the executive director. The executive director has broad freedom to determine the means that will be used to achieve organizational aims.

Advisory Board Model: A board selected and dominated by the executive director. This board provides prima facie legitimacy to the organization but governs only in a nominal sense. Board members provide advice and may rubber-stamp the executive director's recommendations.

Q5. Which model is nearest one to represent your organisation governance model? Which one would you like to be your model?

_____

_____

Q6. Can you suggest a new model with reasoning?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

How does Risk Management relate to Governance?

It is important here that we distinguish between governance and management. Theoretically, they are separate functions. Management is more about the preparation of policy proposals; the implementation of what is agreed and the efficient and effective deployment of resources. Sometimes, governance is used to specify or identify poorness in the system. Without taking into account “Risks”, large, medium and small organisations encountered huge difficulties to survive. Hence, good governance applies it in every aspect of the system. Risk management is a central part of any organisation’s strategic management and an integral part of governance.

To identify and apply any type of risk, dedicated management has been established by the governance to make sure risk predictability is analysed and evaluated. Risk management is

connected with the standards, guidelines and best practice publications. Inadequate risk management and accountability leads to poor governance.

Q7. Are you involved in Risk managements?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q8. Have you thought about Risks may turn the company to failure?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q9. Have you written down a procedure to avoid risk?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q10. Have you presented it to the management? [0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q11. Was it implemented cross the organisation?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

The impact of Risk Awareness on Governance

This study is driving the issue that risk awareness will improve and solidify the efficiency of Risk Management. Hence, governance should reveal the risks to all involved in the process and have it as a transparent element. This research suggests ways and means for implementing the risk awareness to staff. Risk Awareness is a plan for response to incidents, identify system and process weakness. Organizations, whose people are aware of risk they are able to achieve their business goals in a proper way. Organisation with good governance needs to focus to increase awareness of risk to achieve their objectives and goals.

Q12. Were you aware about the Risk Awareness?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q13. From the discussion above, do you think it improves the Risk Management efficiency?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q14. Can you suggest a method on to deploy Risk Awareness?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

The impact of Governance together with Risk Awareness on the organisation success

If the risk is identified at its early stage, there is a good chance to circle the risk and eliminated or the risk is moved to the customer to avoid any legal consequences. This is possible only if the risk has been defined and the governance approved that all staff are aware of it. Governance could analyse the risk by applying it through a simulation model to ensure sustainable solution and success of the organisation. Some literature mention main purposes of corporate governance.

- To ensure the board, as representatives of the organisation's owners, protects resources and allocates them to make planned progress towards the organisation's defined purpose.
- To ensure those governing and managing an organisation account appropriately to its stakeholders.
- To ensure shareholders and, where appropriate, other stakeholders can and do hold boards to account.

Q15. If we tie up Risk Awareness with Governess and apply it to a software model, do you believe it will prevent unflavoured consequences?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Element 2: ENTERPRISE

What is Enterprise?

One definition of the term "enterprise" is a business organisation, an organisation created for business ventures. In other words, an enterprise is a project or a mission that produces products or services. In contrast, another definition of enterprise is "a purposeful or industrious undertaking (especially one that requires boldness or effort to achieve)".

In this research we are concerned with the former definition within which there are broadly two classes, namely, business enterprise (mainly profit making establishments that provide products and services required by the market) and social enterprises (profit or non-profit making organisations that usually provide low-cost or care and charitable community services, such as Red Crescent and Police.

What is Enterprise Risk Management (ERM)?

There are different meanings of ERM but the most appropriate one for this research area is an organisation created for business ventures with the aim of eliminating any risk for itself and other establishments. An ERM setup is a model that incorporates risk minimisations at all management levels, at all times. A feedback mechanism is normally an essential feature of the model that is intended to evolve the model, in order to improve and enhance the detection of any risk manifestations that may initiate or creep in the system silently. Therefore an organisation must plan, organise, lead, and control the activities within, in order to minimize the effects of risk on itself, its capital and earning potentials. Enterprise risk management expands the process to include not just risks associated with accidental losses, but also Financial, Strategic, Operational, health and other risks.

Enterprise risk management is: [link below] 2

• A process, ongoing and flowing through an entity

• Effected by people at every level of an organization

• Applied in strategy setting

• Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk

• Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite

• Able to provide reasonable assurance to an entity's management and board of directors

• Geared to achievement of objectives in one or more separate but overlapping categories

2 http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Q16. Does Enterprise Risk Management (ERM) mean anything to you?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q17. Does your employee understand (ERM)?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q18. Have you had any formal training or induction in existing company policies?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q19. Does your company implement ERM?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Why implement ERM?

ERM effectively enables companies to take more strategic business risk and greater advantage of the opportunities in their core business.

There are five fundamental reasons for implementing ERM [link below] 3

Reduce unacceptable performance variability

1. Align and integrate varying views of risk management
2. Build confidence of community investment and stakeholders
3. Enhance corporate governance
4. Successfully respond to a changing business environment
5. Align strategy and corporate culture

3 http://www.ucop.edu/riskmgt/erm/documents/protiviti_faqguide.pdf

Q20. Do you think it is important to implement ERM?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q21. Which one of the above 5 reasons are implemented in your enterprise? *(Select a number 1-5 from the above list)*_____

ERM and Managers

Enterprise risk management enables managers to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. Enterprise risk management ensures that management has in place a process setting objectives and that the objectives are appropriately resourced and supported. Therefore Enterprise and risk management are tied together. There are different risks facing organisations such as: [link below] 4

1. Hazard risk
2. Liability torts, Property damage, Natural catastrophe
3. Financial risk
4. Pricing risk, Asset risk, Currency risk, Liquidity risk
5. Operational risk
6. Customer satisfaction, Product failure, Integrity, Reputational risk
7. Strategic risks Competition, Social trend, Capital availability

4 http://en.wikipedia.org/wiki/Enterprise_risk_management

Q22. Do you think that ERM can play an important role to deal with risk?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Enterprise risk management encompasses [link below] 5

• Aligning risk appetite and strategy – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

• Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

• Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

• Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

• Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

• Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

These capabilities inherent in enterprise risk management help management achieve the entity's performance and success targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

5 http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

ERM and Risk Awareness

Enterprise risk management and performance management are two complimentary processes essential for the management of an organization. Both disciplines are designed to support organizations' efforts in making decisions and meeting their goals, ERM through the identification and management of those risks that could affect business objectives, and performance management through the identification and measurement of the drivers needed to achieve results.

Large, medium and small organisations need to be more involved in risk awareness. So implementing ERM will give them ability to control, plan and organize that lead to reduce risk. The result will give employees the knowledge and understanding they need to better protect valuable information assets through proactive, security-conscious behaviour. Organisations, whose people are aware of risk, are able to achieve their business goals in a proper way. Risk Awareness must be one of the Risk Management processes because people that are aware of risks will easily identify assessments and evaluate and control or manage the risks. The organisation must maintain its reputation at other organisations and this will do by implement ERM will give the organisation or company more aware.

0= Don't Know
1= Not Applicable
2= Definitely NO
3= Probably NO
4= Probably YES
5= Definitely YES

Q23. Do you think that risk awareness will lead to ERM?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q24. Does your company have risk awareness program?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q25. How do you test the awareness of your employees in the company?

_____

_____

_____

Element 3: COMPLIANCE

Compliance

Good compliance, within an organization, mandates that employees need to observe the requirements of government systems and adhere to the policies in order to reduce any risk. Therefore the organization must follow this strategy by increasing the level of knowledge and skills of employees in accordance with the requirements for compliance.

Q26. To what extent do you think you are familiar with compliance?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q27. Do your employees understand the meaning of compliance?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

In a Compliance Management Systems Handbook (1996), aimed at administrators of national banks, compliance management system has been described as a method by which the organization manages the entire consumer compliance process. This embodies the following:[link below] 6

a. A set of policies and procedures to guide employees' in the adherence of relevant current laws and regulations.

b. An audit function, sometimes referred to as compliance review or self-assessment (fair lending), which entails an independent testing of the institution’s transactions to determine the level of compliance with consumer protection laws as well as the effectiveness of, and adherence with, policies and procedure.

6 (http://www.occ.treas.gov/handbook/cms.pdf)

Q28. Is there any compliance program in your company?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q29. Are you aware of the compliance procedure of the company?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q30. Do you feel the need to be aware?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q31. Have you had any formal training or induction in existing company compliance policies?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q32. Do you think formal training / induction is sufficient to bring an employee to the full level of awareness?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q33. If no, which one of the following alternatives is more suitable?

a) Regular Bulletins

b) Regular Departmental Awareness Meeting

c) Regularly Displaying Posters of important compliance issue

Q34. Is there any procedure that you do to test the compliance of your employees?

[0 1 2 3 4 5]

The relationship between Compliance and Risk Management

Risk awareness is a combination of vulnerability assessment and knowledge management which provides critical input to the risk identification and risk management process (Gibson, 2003). Therefore each organization must have their own awareness to avoid any uncertain events and develop the attitude of what could go wrong.

Any organisation whose employees are appropriately equipped with the understanding and skill to apply government systems and policies will benefit from reduced risks. This will empower them with the ability to identify, assess and control or pre-empt risks by applying formal risk management processes and, thus, contribute towards improving the relationship between compliance and risk management as a whole. Therefore risk management seeks to manage risk around the key products and services that an organization delivers.

Q35. Is there a relation between compliance and risk management?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q36. Is your company aware of the relationship between compliance and risk management?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

The relationship between Compliance and Risk Awareness

Improving the compliance will lead to increased risk awareness – the thesis of this research study. Large, medium and small organizations that have a high degree of compliance, and their employees that possess the necessary skills and knowledge to adhere to the requirements, will improve the Risk Awareness within the organization, as a whole, and thereby beneficially impact on risks.

Q37. Do you think that risk awareness will lead compliance?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q38. Will employees' compliance positively impact on risk awareness?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Element 4: IT GRC

IT GRC refers to a unified, comprehensive, and inter-connected approach towards Governance, Risk Management and Compliance that relates to the organization's use of Information Technology (IT).

The aim of this research is to reduce risk for any establishment, be it public or private organisation, through Risk evaluation. Within the last two decades positive and effective advances have been taken forward towards this goal; for example, large companies have incorporated a dedicated department to handle any risk category that the organisation may encounter during its life cycle. These departments are often referred to as Risk Management Departments.

While the advances in this area are very encouraging they are frequently based upon ad hoc and disjointed processes that are integrated poorly or are lacking in scope. Hence, this research seeks to propose a formal technique which small, medium and large public and private organisation may adapt to their specific requirements, thus leading to a near-free-risk business.

Organisation need to put the three elements Governance, Risk Management and Compliance under one umbrella which is called IT GRC. IT GRC refers to a unified, comprehensive, and inter-connected approach towards Governance, Risk Management and Compliance. It relates to the organisation's use of Information Technology (IT).

Governance requires that decisions are made and implemented using a clear and legitimate process, to achieve consistent and effective policies.

Risk management is a method used to reduce a risk which is unexpected in organisation and it contains the main elements or processes are risk identification, risk assessment, and risk control.

Compliance the requirements of government systems and adhere to the policies in order to reduce any risk.

7 http://www.ecominfotech.biz/governance-risk-compliance.php

Q39. Does IT GRC mean any think to you?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q40. IT GRC Implement in your company?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

IT (Information Technology) can be used as a pillar to support the aim of this research. By default, IT interconnects a company's employees, and perhaps their customers. IT can be used to deliver simultaneously and harmonise multiple compliance requirements to all staff and customers included in this organisations.

Q41. To what extent do you think that IT can interconnect company's employees?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

IT can be used to control the workflows of audit and risk management.

Q43. Do you think that IT can be used to control the workflows of audit and risk management?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q44. Does your company follow this procedure?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

The myriad of regulations and mandates increases the cost of any organisation. The author believes IT reduces the cost of this process.

8 http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Q45. Do you think that IT can reduce the cost of any organisation?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

By harmonising and fairly distributing the up to date regulations to all staff, a feedback can be monitored to automate the process of receiving and understanding/grasping the regulations. The feedback may reflect positive or negative opinions about a specific regulation. In case of negative opinions, an action should be taken to overcome this hurdle. Thus, IT does reduce the risk to the organisation.

Q46. Does your company have up to data regulations to all staff?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

To distinguish IT activities in organisations and explore their success, the following two issues have been selected.

- IT is able to translate risk assessment data into actionable recommendations.

Q47. From your experience do you think IT is able to translate risk assessment data into actionable recommendations?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

- Hence, identification of weaknesses in existing risk management processes is assured.

Q48. What kind of tools is the IT Department using to identify risks?

_____

_____

- Therefore, flexibility to adjust to new or update regulatory requirements is feasible.

Q49. Do you think that risk assessment and identification can measure any organization performance in adapting and responding to risk?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

In the above, the first two criteria were selected as measures of an organization's performance in adapting and responding to risk, while the third was selected as an indicator of their ability to adjust to a dynamic compliance landscape. Companies with top performance based on the above criteria should be exclusively identified as a model for this research.

It is anticipated that the findings of this survey into good practices in IT, that good companies shares several common characteristics which include the following:

- Consistent policies and procedures for IT compliance and IT risk management
- IT vulnerability assessments and IT risk assessments
- Responsible executive or team with primary ownership of IT GRC initiative; communication of corporate policies, practices and expectations for ethical behaviour
- Repository of log, information and event data; of applicable laws and regulations; of risks and related information
- Modelling of interconnections and dependencies of IT risks; of how IT risks impact expenditures and corporate objectives; of impact of unmitigated risk versus cost of mitigation
- Hence, best companies will show that they are managing IT as a strategic asset and adopt a continuous improvement approach to IT GRC

Companies are on the increase to invest on IT GRC. The following set of questions will test this assertion:

Q50

Has the IT in your organisation improved operational efficiencies (reduce total cost)?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q51

Do you think IT activities in your organisation provides enterprise-wide visibility (improve decision-making)?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q52

Do you think Mitigate IT risks (technology, operational) in your organisation are viable?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q53

Has your organisation addressed new / changed regulatory compliance requirements?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q54

Do you think in your organisation has improved security of the IT infrastructure?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Hence, the strategies driving current investments in IT GRC can be defined with the following set of questions:

Q55

Do you think your organisation has established and enforced consistent policies and procedures?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q56

The development / improvement of IT governance framework have been adopted?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q57

Your organisation has developed comprehensive, continues compliance infrastructure?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q58

Your IT has automated risk and compliance processes and controls?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Element 5: RISK MANAGEMENT

Risk Management is an overarching organisational framework intended to protect an establishment from the negative impact of risky incidents which are encountered in their normal course of business. Risky incidents may be characterised as those events that can be detrimental to an enterprise and severely destabilise or critically damage the establishment (e.g. financially or in terms of credibility).

The three main facets of Risk Management are processes that facilitate: i) Risk Identification (the recognition of real potential risks that may endanger an establishment), ii) Risk Assessment (the evaluation of the likelihood of each risk occurring and the level of seriousness of the impact) and iii) Risk Control (the action that the establishment needs to take in order to totally eliminate, or minimise, the incident of occurrence and where it does occur how best to contain the impact to a minimum).

9 http://www.islamicity.com/articles/Articles.asp?ref=TI1004-4144

Risk Identification

Risk Identification is the identification of real potential risks that may impact on the establishment to its detriment (i.e. its business, resources, staff or its clients). Enterprises are encouraged to develop their knowledge and capability to properly recognize and identify all major risks that they may encounter in the normal course of their business. Examples include fire, data security, burglary or industrial espionage.

Questions that need to be answered during the process of risk recognition and identification are:

1. What could go wrong and what are the likely consequences?
2. What needs to be controlled or implemented to prevent error?
3. What misfortunes have other organisations experienced that should be catered for?
4. What must go right?

Borodzicz (2005) suggested Risk Identification involves listing and reviewing every type of risk that an organization might conceivably face.

Risk Assessment

In a simplistic model involving fire risk, Risk Assessment would involve, firstly, an assessment of the likelihood of a an outbreak of fire (e.g. 5 on a scale of 1 to 10) and

secondly, an assessment of the impact of such an occurrence (e.g. person trapped or loss of life in building or valuable data being destroyed) again using a similar numerical scale (e.g. 4). A very simplistic overall Risk Assessment for this example may involve computing the product of the two assessments to determine the real level of risk involved, namely an overall risk assessment of 20% (which may be regarded as low risk).

While this example is indeed relatively simplistic, it does illustrate the relevant methodologies but the actual algorithm and computation used would typically be determined, based on the set of rules and regulations laid down by the Risk Awareness officer and strongly influenced by the particular needs of that industry/service.

Thus all potential risks identified for an enterprise should be evaluated on a similar basis in terms of:-

The probability (or likelihood) of occurrence of the particular risk, and

The impact (or severity) of the consequences in the event that the risk is experienced.

Each risk will, therefore, be individually quantified in terms of a statistical aggregate of the two assessments which may be used for prioritising within the Risk Management framework.

Risk Control

Risk Control (ideally) determines the action required to totally eliminate the incident of a risk, based on the Risk Assessment made above. However, as nil-risk is unrealistic, it is more concerned, firstly, with specifying the preventative measures which are required to minimise the probability of occurrence and, secondly, if it does occur the remedial actions are to be applied to best contain and limit the impact of the incident.

Why is Risk Management important?

Risk Management is intended to manage risk surrounding the key products and services that an enterprise delivers, in order to safeguard its interests as well as those of its clients. ***It may be described as the process of*** identifying and analysing the risks faced by an organisation and accordingly introducing organizational capabilities to respond appropriately in the face of risk manifestations. The process is inherently intended to be evolutionary and makes provisions to incorporate, into the framework, other previously unforeseen risk factors that

become known through own misfortunes within the enterprise or the unfortunate experiences of other enterprises.

It is prudent for any organisation to protect their services, resources, employees and clients against all risks that can arise in the course of daily business in order to improve their performance by contributing to:

- Increased certainty and fewer unpleasant surprises
- Better quality of service
- More effective management of change
- More efficient resource utilisation, and
- Better management at all levels through planned decision making

Risk Management is an overarching senior management function which determines the degree of uncertainty, or risk levels, that an establishment shall afford to take in the quest for greater profitability, shareholder value, and indeed quality of service.

Human Resources of an organization are involved in usage, operation, and maintenance of the IT resource. Therefore individuals who are the most vulnerable part of any plan or effort to minimize the risk potential from IT in an organization which has been highlighted by audit reports, periodicals, and conference etc. Hence, IT risk management should involve tackling the problem of insufficient awareness through different organizational programs, training etc.

Q59. To what extent do you think Risk Management can reduce the effect of IT risk?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q60. Does your enterprise have a risk Management Policy?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q61. Are you aware of the list of identified risks?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q62. Are there notices/posters or memorandum sent regularly to staff members to keep them informed of the list of risks?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q63. In what form is the information disseminated to staff?

_____

Q64. What way do you feel is most appropriate for effective, and inexcessive, information disseminated to staff?

_____

_____

_____

Q65. Are staff members actively consulted and encouraged to contribute ideas in connections with risk identification, assessment and control?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q66. How confident are you about the coverage and significance of the identified risk categories?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q67. How confident are you in assessment ratings of the identified risk?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q68. How confident are you in policies and procedures defined for control of risk (i.e. pre-empting the occurrence of risk and limiting the impact of risk?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q69. If any of the last 3 questions are rated < 5(high) have you, or anyone else, notified the management of the reasons why you do not have full confidence on any aspect?

[0 1 2]

0= Don't Know
1= Yes
2= No

Q70. Were suggestions followed up (irrespective of whether finally adopted or not) and was feedback given to the relevant staff member/s?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q71. During the last 12 months, how often has ANY form of risk alert been triggered within your Department?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Element 6: RISK AWARENESS

The importance and role of Risk Awareness within an enterprise is widely recognised today among the wide ranging types of enterprises (large, small, profit- and non-profit making, service and manufacturing businesses). According to a report in Continuity Central website[link below] 10, recent research conducted by Aon (2009) revealed that "*70% of UK risk managers have declared that making sure the employees in their organisation are 'risk savvy' is their biggest challenge*". The risks faced by companies have increased dramatically in range of categories and number of incidents that it is considered significant enough that they "*... need to be dealt with by employees throughout the organisation...*" and not just by senior managers alone.

10 http://www.continuitycentral.com/news04361.html

Risk Awareness is a combination of *vulnerability assessment* and *knowledge management*, which provides critical input to the Risk Identification process within the overarching Risk Management framework (Gibson, 2003). Therefore, each enterprise must develop their own awareness schemes and policies to identify and understand what could go wrong, and additionally develop crisis management strategies, particularly for unforeseen negative incidents.

Thus, Risk awareness is a mechanism intended to facilitate repaid response to manifestation of negative incidents through the reliance of practical knowledge and shrewdness of all staff members. Such capabilities rely on some understanding of human factors as well as products and services being provided. Employees will be capable of recognising and responding to early signs of impending crisis, or be informed enough to play their respective part in a more sudden manifestation of crisis.

Getting to this stage involves responsibility at a high level management for the formulation of policies for action and crisis handling. However it is paramount that risk classes and such policies are communicated reliably throughout the organisation. Thus a reliable structure for the dissemination of information regarding risks, policies and procedures is to be established. This can take one or a combination of a number of methods (e.g. regular reports of risk incidents detected, memorandum, email, regular induction and updating courses, etc), and as such requires reliable management through departments such as Human Resources.

Why is risk awareness important?

Risk awareness is important so that all concerned are clear what threats prevail, how to recognise early signs of these, what course of action to take to prevent it aggravating and what action to take if the worst happens and facing with a full blown crisis is really

unavoidable. It is also necessary so that staff members within an organisation clearly understand that certain actions taken by themselves (whether knowingly or inadvertently) may expose the organisation to serious unnecessary risks and may further result in disciplinary action being initiated against staff member/s, thus inducing some level of self control and responsibility concerning deeds and actions permissible among the staff members themselves.

Types of awareness

Human awareness includes the ability of people to recognize risks on the basis of their own experience and that of others. In addition individuals should be encouraged to assess the same (or similar) risks in their own private lives to develop as sense of constant risk awareness beyond the boundaries of their employment. Such experiences would be shared by staff for the well being and benefit of friends and colleagues – this is called *awareness of the self and awareness of other people* (Markova, 1987). In a similar way, *cultural awareness* is the term used to describe behaviour of language use and communication (Tomalin, 1993).

Achieving risk awareness

The characteristics that staff needs to be aware of risk include skills, culture and appreciation of the importance of Risk Management:-

Skills: Communications skills are required to facilitate cooperate between individuals for mutual benefit, including the exchange of knowledge of known skills and best methods for avoiding or dealing with risks. Levels of attainment in Risk Awareness is essential for success thus, individuals need to be carefully selected for special training (e.g. Fire Marshals) through whom information and remedial action can be disseminated to other staff who may be less able to cope with such matters of improperly motivated in that respect. This will improve the awareness of risk.

Culture: An organization needs to have a culture to stimulate and encourage new ideas and to have control over the way people behave. It helps to produce a feeling of motivation. There are a number of characteristics of a culture that can help to raise risk awareness in organization such as good organizational learning, high job satisfaction, a challenge process, appropriate human resource practices and quality training in Risk Awareness (Hillson, 2003).

Importance of Risk Management: People need to know why Risk Management is important because this knowledge will help to raise awareness of what risk is and the the principles and policies of the Risk Management process of their organisation.

First some More general questions:

Q72. Is there a policy guideline within your department for Risk Awareness?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q73. Are you fully aware of all risks and remedies that may affect your organisation?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q74. What kind of tools do you rely on to update yourself?

[0 1 2 3 4] if other please specify _____

0= Don't Know
1= None
2= Dept Meeting
3= Word of Mouth
4= Other (please specify)

Q75. Do all employees within in your department have the same opportunity to become equally aware of the risks and remedies, as yourself?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Q76. Has training been provided in your Department on the risks and remedies?

[0 1 2 3 4 5]

0= Don't Know	**(Answer not known)**
1= Not Applicable	**(not a relevant question)**
2= Low	**(or Definitely NO)**
3= Low-Medium	**(or Probably NO)**
4= Medium-High	**(or Probably YES)**
5= High	**(or Definitely YES)**

Second some more specific questions: Now please spend a little thought and time to answer the following questions as accurately as you can.

Q77. Is there a clear Health & Safety policy defined for your organisation/department?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q78. Do you know precisely where the policy document may be retrieved right now?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q79. Are you confident that the policy document you have access to is the latest revision?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q80. Does the policy cater for Fire risk?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q81. Does the policy cater for Sudden Illness?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q82. Does the policy cater for Electric Shock?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q83. Does the policy cater for other Disasters (natural or artificial)?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q84. Does the policy cater for unauthorised individuals within your department?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q85. Is there a First Aid or Recovery area in the premises?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q86. Are there Medical/Nursing staff on the premises?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q87. Do you know the internal emergency telephone number?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q88. Is the emergency number different from within the organisation?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q89. Do you know where the emergency FIRE ALARM actuator is?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q90. Do you know where the nearest Fire Extinguisher is located?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q91. Have you spent any significant time reading the instructions on the fire extinguisher?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q92. Do you know how many different types of fire extinguishers there are (and their uses)?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q93. Do you know precisely where the nearest EMERGENCY EXIT is right now?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q94. Do you know who your Fire Marshals are?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q95. Do you know where to locate at least 2 Health/Safety Marshals in an emergency?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q96. Do you know where the meeting point is after an emergency building evacuation?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q97. Are you confident that you know what actions to take if a fire is burning outside your room door and your escape route is blocked?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q98. Does your organisation run formal First Aid Training?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q100. Does all/some staff receive this training?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q101. Have you been offered the opportunity to train as a First Aider?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q102. Are you confident about what to do in the event of natural/artificial disasters (earth tremor, hurricanes, severe storms etc)?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q103. Are you confident that you are aware of ALL types of risks in IT and their impact on you and your organisation?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q104. Do you know what a TROJAN is and its impact?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q105. Do you know the difference between SPAM and SCAM?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q106. Do you know how any of the above two threats can occur?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q107. Can you distinguish between Adware, Freeware and Shareware?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q108. Can you distinguish between Internet, Intranet and Ethernet?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q109. Do you know that your computer can be hijacked by hackers and misused?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q110. Are you aware of the dangers of using passwords that are based on family names, date-of-birth and similar choices?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q111. Are you aware of dangers of using everyday language words as passwords (just because they are easy to remember)?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q112. Are you aware of the dangers of using overly complicated passwords?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q113. Do you realise that your desktop computer typically has more than one user account?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q113. Are you aware that a person having access to an administrator account can easily examine your user account data, email, files etc?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q114. Your computer reports that your FIREWALL is off. Do you know what the implications are?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q115. Your computer reports that your ANTIVIRUS software is out of date. Do you confidently know the real risks or how to update it?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q116. Your computer reports that your HDD appears to have been corrupted. Are you confident of what the seriousness of the message?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q117. Your system suffers a catastrophic system crash. Are you confident that you can recover your data with the minimum loss (e.g. 1 day loss)?

[0 1 2 3 4 5]

0= Don't Know (Answer not known)
1= Not Applicable (not a relevant question)
2= Low (or Definitely NO)
3= Low-Medium (or Probably NO)
4= Medium-High (or Probably YES)
5= High (or Definitely YES)

Q118. Is your data backed up regularly?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q119. Are you aware of the benefits/dangers of not backing up your data?

[0 1 2 3 4 5]

0= Don't Know
1= Not Applicable
2= 1200 KB/s (or LOW)
3= 2400 KB/s (or LOW-MEDIUM)
4= 4800 KB/s (or MEDIUM-HIGH)
5= 9600 KB/s (or HIGH)

Q120. Your organisation has been broken into during the night and several computers are stolen. State what the risks are arising from the theft: _____, _____, _____, _____. (list as many as necessary)

Thank you

Would you like to receive feedback after the analysis?

☐ Yes

☐ No