# MANAGING RISK IN INFORMATION SECURITY, KNOWLEDGE TRANSFER AND CORPORATE CULTURE SHOCK IN GOVERNMENT SECTOR CASE STUDY

## TABLE OF CONTENTS

# 1. DEFINITION & MAPPING OF RESEARCH QUESTIONS

A study on *managing risks in information security, knowledge transfer and corporate culture shock* in government sector case study is a broad and well informed topic for study. As can be seen, this topic has broad elements from which the research questions will be mapped and defined. The topic touches on management aspect, risk, information security, knowledge transfer, and corporate culture shock. The study will rely on these elements to develop research questions. Management as an aspect of the study topic suggests that the research questions should address different managerial approaches employed in the public sector to overcome the problem of risks in information security, knowledge transfer and corporate culture shock. Management deals with various elements in an organization including processes, resources and people. This suggests that the research questions will address how the public sector manages processes, resources and people, as key steps in managing risk associated with information security, knowledge transfer, and corporate culture shock.

Risk being an element in the study topic suggests that the research questions will identify potential types and sources of risks in information security, knowledge transfer and corporate culture shock. Merging management aspect, information security, and the risk suggests that the a broad area for the study question will address how various levels of management in the public sector manage risk in information security, knowledge transfer, and corporate culture shock. Knowledge transfer refers to how skills are transferred from one employee to the other. Knowledge transfer can also happen between different departments or ministries in the public sector. Thus, risks that will be addressed by the research questions are associated with human resource development. Corporate culture shock is associated with how organization adapts to new environment. This study understands that the public sector relates with both private and foreign sectors to achieve its goals; a condition that can trigger corporate culture shock. In this view, the study questions will address how the public sector manages risks associated with her relations to the private and foreign sectors. The study also understands that the public employees can be transferred from one ministry to the other, thereby forcing them to adapt to the new work places and culture. Therefore, the study questions will address how the public sector manages risks related to employee transfer.

## 2. INTRODUCTION

This study will be focused to explore the topic of managing risk in information security, knowledge transfer, and corporate culture shock. In the context of the study topic, the following chapters will constitute what the proposed study:  organisation & management context, problem and issue description, literature review, research questions & objectives, discussion of documents three, four and five, research plan and methods, ethical issues and organizational political issues, and outcome. Organisation and management will throw more light on *what, who and how* management is viewed in regard to the public sector. Problem and issue description will discuss what motivated this study. The rationale behind the study will be presented in relation to risk management in the public sector. In addition, the chapter will show why it is important for this study to be conducted owing to benefits that it will bring to various stakeholders in the public sector services.

Once, clear reasons on what and why the study should be conducted, there will be a chapter on literature review, which covers various aspects of risks management, but within the scope of research topic. The literature review, together with the problem and issues to be resolved in the study will be used to form well-informed research questions and objectives. In this regard, the study will reflect on how research questions are defined and mapped in the first chapter of the paper. The next chapter will be a discussion of documents three, four and five. These documents will show how the study will develop and implement data collection and analysis tools. In particular, the chapter will show how qualitative and quantitative research tools will be developed and employed at various stages of the study.

The research plan and method chapter will address how the study will show how the researcher plans to complete the study in regard to time allocated for every process in the study. The chapter will further show how the researcher considered various research methodologies from which a strong methodology will be chosen for the study. The chapter on ethical issues and organizational political issues will address how the study plans to consider and treat various ethical requirements in the study. In particular, the ethics of access to corporate information, permission, and consent of respondents will be discussed. The last chapter will briefly describe the study outcome at both personal and organisation level.

# 3. ORGANISATION & MANAGEMENT CONTEXT

The public sector, which the study focuses on, is viewed as an organisation. An organisation refers to not only people but also processes and resources engaged in to achieve common goal. The study understand that in the public sector, there are resources and process as well as people charged with the responsibility of ensuring that information security and knowledge transfer are effectively handled to avoid risks that would jeopardise their quality. The study understands that culture shock is a phenomenon that impacts on organisation operations hence limiting its success. The public sector organisations have various categories of employees not only in the departments they work but also their ranks. Departments are many and this study will select only those which can provide the required number of respondents and relevant data needed for the study.

The study understands that management is an aspect of public sector organisations. Managers are of various categories, and the study proposes to use all of them. The senior-level management, middle-level management and lower-level management will be significant in the study. Management is executed in different departments in the public sector organizations. For the purpose of the study, only managers from departments that are associated with information security, knowledge transfer and culture shock management will be considered. Management is also executed on human being, resources or processes. The researcher intends in this line to consider key personnel, resources and processes involved in the management of risk in information security, knowledge transfer and culture shock.

## 4. PROBLEM AND ISSUE DESCRIPTION

The problem, which is the central issue in the study, is risk management. The issue is expounded to cover its wider dimensions in regard to information security, knowledge transfer and culture shock. Information security is a sensitive issue that organisations have invested a lot of money. This is to prevent intentional or intentional leakage of organisational information. This trend has also been witnessed in the public sector across the globe with a view to prevent its socio-economic disadvantages. For instance, leakage or public information to either private or foreign sectors makes these sectors know the top government secrets, which can result in socio-economic instabilities. The study acknowledges that risks in information security results from poor management processes and resources. Problems usually emerge once such risks are not properly managed. Hence, a study that focuses on how this type of risk is managed in the public sector will be beneficial not only to the organisation but also other stakeholders in the public sector services. A study that focuses on managing risk in information security will ensure that the public are informed about performance in the public sector. The study will help the relevant managerial personnel to identify what is expected of them and what is not expected of them to keep the public sector information secret.

Knowledge transfer is understood as a concept that is associated with risk due to involvement of people and other sectors in the public service. The public sector organisations usually engage employees with different skill and competence levels. There are senior employees with many years experience and skills and junior employees with a few number of years' experience. When these employees brought together to deliver towards common goal, there must be skill-gaps between the two categories of employees. This can present much problem especially when the junior are not willing to transfer the knowledge they have to their juniors. Employees can be of the same experience and skills but work in different departments within the public sector. The employees may not feel like sharing their knowledge with other employees from another department, thereby resulting in problems that impact the overall operations and delivery of the public sector. A study that focuses to explore how management of risk associated with knowledge transfer will therefore help the public sector management to identify their weaknesses and strengths that can be used to enhance future integration of employees' skills in the sector.

Corporate culture shock is acknowledged as a problem that usually comes when an organisation tries to adjust and adapts to a new operation environment. In the public sector, this problem is quite common due to employees’ transfer and inter-sectoral collaboration. Public employees are transferred to work in different ministries based on national needs. This transfer requires employees to adapt to the new ministry’s processes, policies, people, and resources. In some cases, employees find themselves not able to co-operate with the new work environment hence resulting into problems that impact on the organisation’s performance. Employees of such nature have low work morale and job satisfaction, which is detrimental to their lives. Corporate culture shock in the public sector can emerge from her relations with both private and foreign sectors in delivering its services to the general public. The organisation shock can be experienced when the public sector tries to accommodate or adapts to the demands of the other sectors. The public sector finds problem with the relations hence causing further problems in delivering to the citizens. A study that focuses on how the public sector manages risk in corporate culture shock will therefore be significant in preparing the public sector to work with other sectors without negatively impacting on her deliverables. The public sector will also identify where they have failed to develop high work spirit among her employees.

Based on the elements of the study topic, the study acknowledges that information, employees and other sectors are significant in helping the public sector deliver its roles to the citizens. However, poor management processes of public employees, information security and corporate culture shocks can lead the country into socio-economic crisis. It is in this view that the study proceeds to evaluate how risks associated with these elements are handled in the public sector in order to help improve the situation.

## 5. LITERATURE REVIEW

Extensive literature review is one of the research activities that made this study successful. Based on the research topic, information security, knowledge transfer and culture shock are all dependent on organizational data and information. Thus, a review on data security was necessary. Human beings uses organisational information to achieve the required security thus the study conducted a review on various organizational controls to show how management can integrate them into organizational operations.  In brief, this review proceeded to explore the study topic through various chapters of information risk management, knowledge transfer and corporate shock as detailed from the next chapter.

### 5.1 Conceptualization of Risk management

This study conceptualised risk management in different ways though based on what other studies show. The study conceived that risk management is a complex and involving task that needs efforts of the entire organization right from individuals, middle management and senior executive (NIST, 2004; CNSS, 2010).  Based these publications (NIST, 2004; CNSS, 2010), it could be noted that whether the risk management is needed in information security, knowledge transfer or culture shock, the ultimate requirements is that the top level management needs to provide strategic vision, goals and objectives for the entire organization while middle-level management taking a responsibility in planning, implementing and managing projects. This implies that individuals in the lowest level are also key in achieving effective risk management since they are the ones who interact with the organizations systems and resources that support organization's missions and business functions. Thus, this study therefore strongly considered that employees from different corporate levels in the government sector form part of participants.

### 5.2 Components of Risk management in Information Security, Knowledge Transfer and Culture Shock

Management of risk cannot be achieved without considering it potential components. In this view, the study reviewed some of the internationally recognised components that can cut across all government sectors. To begin with, risk-framing is the first component in managing risk regardless of its type (Special Publication 800-53A). This process deals with how an organization establishes a risk context. In this regard, the management needs to describe the environment that calls for risk-based decisions so that they develop a risk-management strategy. In this strategy, organizations needs to stipulate how it intends to assess potential risk, respond to risk and monitor risk (Bayer and Maier, 2006). Therefore, this study argued that good framing of risk with effective assessment, response and monitoring strategies would help the government sector to manage risks that are associated with information security, knowledge transfer and organization culture shock.

The importance of developing risk framework can be acknowledged during risk assessment. Here, risk assessment needs to be carried out within the organisation risk framework with the focus to identify threats to the organisation (CNSS, 2009). In this view, this study argued that a good risk framework would help the government sector to regulate the scope of risk assessment, thereby revealing specific and unique harm, internal and external vulnerabilities as well as the likelihood that the harm will occur to the organisation. The threats, internal and external vulnerabilities can be identified through such strong risk framework and assessment but it can still be hard if the organisation has poor response rate. Therefore, this led the review to another component called risk response (E-Government Act, 2002). This component aims to provide a consistent firm-wide response to risk based on the risk frame.

Even though implementation of best course of action may be successful, it is highly recommended that the organization carries out risk monitoring (ISO/IEC 27001, 2006). Analytically, risk monitoring can help an organisation to ascertain that planned risk response measures are executed. It can also help in ensuring that the requirements of information security derived from organizational missions, directives, policies, standards, guidelines, federal legislations, and regulations are satisfied (ISO/IEC 27001, 2006). Based on these benefits of risk monitoring, this study reasoned that in monitoring risk in information security, knowledge transfer and organization culture shocks, it would be imperative to reflect on both internal and external influences. Risk monitoring also helps to determine the effectiveness of ongoing risk response measures after implementation and to identify risk-impacting changes to the information system and its operating environment.

## 5.3 Managing Risk in Knowledge Transfer

The previous chapters present general information on risk management that cut across all the topic elements. Therefore, this study narrowed down to review on how risk in knowledge transfer can be managed. There are three risk factors associated with knowledge transfer (Szulanski, 1996). First is the causal ambiguity of knowledge. Second is the reduced integration ability of the recipient. Third is the emitter-recipient communication. Thus, in the view of this study, the management needs to recognize the above processes to ensure that the knowledge is secured. In particular, the management needs to reduce chances that the three causes would occur during knowledge transfer. In this view, it can be noted that integrity and authenticity are key in effective knowledge transfer or else the objects or subjects involved may be avenues for risks.

In deliberating the aforementioned checks and balances, it should be acknowledged that knowledge security encompasses protection of the data, information and the knowledge, which forms the intellectual capital in a knowledge-based society (Argote, McEvil and Reagans, 2003). This process is quite significant to achieve high competitiveness of the organization. Logically, it can be seen that knowledge and information are closely related that poor management of risk affecting either of them can lead to poor management of risk in the other and vice-versa.

Information security needs to meet three objectives. These are confidentiality, integrity and availability (ISO_27001 Standards, 2008). Even if these can be regarded as the core objectives of managing risk in information security, it can be argued that they play significant role in ensuring that the knowledge transferred does not experience threats that can induce harm to the organization. Confidentiality seeks to ensure that knowledge being transferred is only accessible to only authorized individuals. Integrity seeks to ensure that the transferred knowledge maintains its original accuracy and completeness. Availability seeks to ensure that transferred knowledge is interruptible accessible to authorized individuals. In brief, it can be leant that knowledge security can help to secure not only the knowledge assets and processes involved but also the technologies, and human factors involved in the transfer of knowledge.

One of the most threats in information and knowledge transfer is leakage of information, which affects intellectual property of the organization (ISO_27001, 2005). In view of this threat, this study argued that the organization should embrace proactive strategy in identifying the vulnerabilities over the knowledge assets particularly in a collaborative work environment to develop efficient and dynamic security policies. However, this should depend on the category of knowledge that is being transferred. Two major categories of knowledge transfer are internal and external transfer (ISO_27001, 2005). Internally, knowledge is transferred within the organization. Externally, knowledge is transferred between the organization and external entities. This suggests that addressing these risks may seem to be different. In particular, it is the organization employees who initiate transfer of knowledge, which may be as a result of lack of awareness of the value of transferred knowledge or due to opportunistic behavior of the employee (Markus et al., 2003). For instance, an employee may intentionally or unintentionally decide to share organizational knowledge with employees of another organization. Therefore, good awareness on the value of organizational knowledge can help to reduce such threats.

Despite whether knowledge transfer is internal or external, absence of trust is one factor that can bring potential threat (Blebea, 2011). Therefore, this study purports that trust should be developed over long period of time to achieve two things. First is to positively influence willingness to transfer knowledge. Second is to positively influence mutuality of the transfer. In this view, it can be noted that lack of willingness and mutuality between organizations can threaten successful knowledge transfer. In the context of internal transfer, an employee would not be willing to share the knowledge he/she possess with a colleague due to lack of mutual understanding and trust between the two persons. Hence, it is advisable for organizations to take long time with the other party to develop these pertinent elements. Logically, this can ensure that the intended intention of knowledge transfer is achieved and exploitation of unintended knowledge transfer is minimized.

Apart from the absence of trust, another risk in knowledge transfer that needs proper management is incompatibility, which arises from institutional differences with regard to their business practices and cultures (Cummings and Teng, 2003). Employees in an organization may come from different cultural backgrounds. Hence, this can impede knowledge transfer with regard to how the knowledge is conveyed, received and interpreted. Analytically, incompatibility can lead to failure in communicating the knowledge information hence leading to devastating consequences. In this view, it is imperative for an organization management to adopt a multi-cultural management approach to identify how various employees can be teamed together for purposes of transferring their work knowledge to others. On this note, knowledge transfer between organizations can fail due to organizational cultural differences. In this regard, it is imperative for the management to understand the culture of another organization before knowledge is transferred so as to reduce negative effects that may arise from misinterpretation or re-contextualization of the conveyed knowledge.

In the transfer of knowledge, close consideration should be given to availability of the required infrastructure (Sveiby, 2000). Thus, this would be key to this study to identify how it impacts on information risk management in the government sector. In this context, lack of physical closeness between the parties involved in information transfer can pose serious threats to transferred knowledge. It is required that an organization fosters geographical proximity of facilities, employee rotation, and joint productions (Sveiby, 2000). In the view of this study, establishing close proximity can enhance face-to-face meeting, transparency and observability of the knowledge being transferred. This would be significant even to the operations of public sector owing to the fact that transferred knowledge can lack clarity and certainty if facilities for the knowledge transfer or information security are set far apart.

As the world trends towards internationalisation and globalisation of corporate activities, it was imperative for this study to review how this can impact on government sector. In the context of the Special Publication 800-53, organizations can use collaborative information systems to discourage occurrence of risks that emerge when facilities are set afar. However, this process needs strong access controls to prevent further risks of unintended knowledge transfer (NIST, 2011a). Thus, this study noted that different tiers of information security management must come into play owing to the fact that not all the tiers in information security management would have equal access privileges. In the context of security requirement of an organisation, this study further argued that risks associated with knowledge transfer can be controlled by substituting or improving security levels of systems used.

In as much as collaborative systems can be used to increase the number of channels for knowledge transfer, this study reasons that it can reduce controllability of transferred information and knowledge. Hence, this can increase chances of unintended knowledge transfer. For instance, use of social media improves communication among employees and organizations though it can either intentionally or unintentionally leads to leakage of knowledge to unintended parties (NIST, 2011a). In this regard, a proper education would help improve the trust that the system would be used for the right purpose for which it is expected within the knowledge transfer. Moreover, it can be argued that education can help to establish a shared understanding on ethical knowledge transfer.

Employees need to be educated on the dangers of transferring their intellectual knowledge or organization knowledge with an external party instead of stating them in the organization risk management policy (Maiwald and Sieglein, 2002). Therefore, this study argued that the organizational management should embrace protective measures against risks of unintended knowledge transfer. In addition, the measures need to stipulate policies that should be observed during information and knowledge transfer. The measures should also address the types of knowledge that can be transferred to another partner. Analytically, if these measures are not put in place, then it is likely that employees can generously share knowledge or retain the knowledge that they possess. Moreover, mitigating measures against risks in knowledge transfer can be embedded in the organization policies.

In the context of information security policy, employees should be made to understand how they are expected to behave when using organization assets and unwanted effects that may arise from unauthorized use of organization assets (McCumber, 2005). In the case of inter-organization relations, the policy needs to explicitly identify areas where knowledge transfer is allowed and how to conduct such knowledge transfer. The inter-organizational agreement policy can also be used to regulate the extent to which the transferred knowledge can be used beyond the agreement. Hence, this can reduce the risk of knowledge spill-over as already noted in previous chapters of this review. Finally, gatekeepers can be used to control the risk of external knowledge transfer (Office of Management and Budget, 2000). In the view of this study, this can reduce the risk of unintended knowledge transfer.

### 5.4 Multi-Layered Risk Management

Risk management, despite its nature, ought to follow a three-tier approach including organizational level, mission/business process level, and information system level (ISO/IEC 27005, 2005). This suggests to this study that management should be conducted across the three tiers with a goal to achieve continuous improvement in risk–related activities as well as to achieve effective communication within a tier and between the tiers. In this way, this study argued that all stakeholders should develop a shared interest towards risk control and reduction. Analytically, one eminent point here is effective communication, which should be embraced by all stakeholders in the organization to control and reduce, if not avoid, risks associated with information security, knowledge transfer and corporate culture shock.

In the corporate perspective, the management needs to frame potential risks and provide the appropriate contexts for all risk management carried out by the firm (Solomon and Chapple, 2005). The second tier addresses risks from a mission/business process angle. This tier should be implemented based on the behavior and operations of tier one, which provides the context of the risk as well as decisions and activities associated with the risk. The last tier entails addressing risk from the information system perspective, which should be informed by risk activities, risk context and risk decisions in both tier one and tier two firms (Solomon and Chapple, 2005). What all this implies to this study is that lack of cohesive approaches and integration between the tiers can be a potential risk hence should be avoided at all cost.

## 5.5 Ultimate Risk Management Elements

Managing risk in information security as well as in knowledge transfer and organization culture shock agree on one thing that the processes involved ought to begin with addressing the CIA triad (McCumber, 2005). The acronym CIA refers to Confidentiality, Integrity and Availability of data as already been reviewed in the previous chapter. A good security management program should commence with proper policies and must incorporate insights from all senior leadership in the organization (Maiwald and Sieglein, 2002). This suggests to this study that a review of information policies in the government sector can be used to achieve some of the objectives of this study in regard to risk management, knowledge transfer and corporate culture shock. In developing good information security policies, the Information Security Office (ISO) should be involved to communicate with all legal departments, business units, and other key personnel (Special Publication 800-37). This will ensure that risks, emerging from information, knowledge transfer or organization culture threats are effectively dealt with.

As a central player in the risk management in information security and knowledge transfer, the ISO mission should be explicitly written out and understood by the staff (Maiwald and Sieglein, 2002). However, this office is not the only responsible body for all malicious attacks on organization computers/information system. Thus, this study noted that ISO exists to help in managing security risk to organisational information and knowledge.

### *The Information Security Office Staff*

Being a technical office**,** Krutzand (2001) states the ISO staffs should possess elementary knowledge of networks, various operating systems, and software development. This study argued that having basic knowledge of these technical elements can enable an organisation have good background understanding on potential risks to organisational information and knowledge. The ISO staffs need to be professionally certified (Federal Information Security Management Act, 2002). This implies that in going about this study, the researcher would be interested in how government personnel in charge of information security and knowledge transfer are certified in CISSP (Certified Information System Security Professional) and CISA (Certified Information System Auditor) (ISACA, 2005). In looking for these certifications in the government sector, key concerns will be taken to prove whether the government employees understand key concepts of risk management in information security and knowledge transfer. Moreover, this study will be interested to establish whether government employees, who are charged with the responsibility of information security, are competent to demonstrate and apply technical skills to solve real world information risks.

Another requirement in a security staff officer is the possession of good presentation and consulting skills (Maiwald and Sieglein, 2002). Analytically, these skills can serve important purpose in interacting with other employees in case a risk occurs. Besides, these skills can help during training sessions. Hence, it can be seen that putting presentation and consultation skills as key to security would not only help in managing information security risks in government sector but it would also ensure that risks associated with poor knowledge transfer are minimized. The security staffs need to show good level of competence and ability to discuss security attacks with other technical system administrators (U.S. General Accounting Office, 1999). This will ensure that effective security policies are enforced to safeguard unauthorized access and dissemination of organizational information and internal knowledge.

### *Security Policy*

Even though much has been said about security policy, it worth to note organizations need to put in place policies to form strong background for organizational information security (Siponen, 2002). The most basic policy that helps in managing risks in information security is the *Acceptable Use Policy*. This policy informs employees what is unaccepted and what is accepted (Siponen, 2002). Logically, this policy would ensure that an organization gets easy time to discipline employees who may abuse information or knowledge that belongs to the organization or individual within the organization.

### *Data Classification*

Data classification is a pertinent component of security policy, which should explicitly provide data classification guidelines to help employees know the types of data that can be shared or transferred, and which cannot be shared or transferred based on their nature (ISO/IEC 31010, 2010). Within the context of CIA triad, data can be rated as high, medium or low based on the sensitivity of the data (Stoneburner, Goguen and Feringa, 2002). In an effective management of risks in information and knowledge transfer, it is a requirement to protect data with high or medium sensitivity. Thus, this study is interested to identify various classes of information in the government sector and how they are managed based on their broad classes.

Apart from proper data classification and the use of *Acceptable Use Policy*, there are three categories of controls that can be used to manage risk in information security and knowledge transfer. These are management control, operational control and technical control (Baskerville and Siponen, 2002). Logically, these controls can help in developing risk management plan and assessment plan. There are four key components of successful security plan (Harris, 2002; Texas Administrative Code, 2002; Swanson 1998; Krutz and Vines, 2001). The first element is classification of data as already been discussed in the previous chapters of this review. The second component is management controls. This second element addresses controls that organizational management is responsible for. The third component is operational controls, which represents daily operations of systems as well as those operations that are most likely to be acted on by a human being. The last component of security plan is technical controls. This last component refers to automated computer applications.

### 5.6 Management Controls

Management controls focus on the management of IT security system as well as the management of risk for a system (Swanson, 2001). The management should be able to assess risk within its own dimension so as to decide whether to accept the risk or mitigate it through various controls. With the existence of ISO in an organization, security of information can be achieved by consulting with data owners. Primarily, the owners of data in this study would be government bodies. In another view, the data owners can be those organisations and various business units, which government sector interacts with in delivering their services. Thus, the management should desist from a common misconception that the IT-department and personnel are the owner of organizational information (NIST, 2009). Instead, the IT officials should be there to cooperate in making the needed information or knowledge available. Therefore, this study will go beyond the IT-department and its personnel to arrive at comprehensive findings.

Even though risk management in information security entails many activities, the organization management is charged with key mandate to ensure that things are straight from the start (Mitnick, 2002). The management needs to demonstrate strong commitment to deliver in agreement to the security plan. The following are three tasks that management should exercise their control so as to reduce, if not eliminate, risks associated with information security, knowledge transfer and organization culture shock.

The management needs to review security controls, manage risk in the life cycle of information system, and conduct a disaster recovery/ business continuity plan (ISO/IEC 31000, 2008). Analytically, a review of security controls in the government sector would be significant in keeping the management aware of the kinds of security controls that should be applied to mitigating a risk. Every department needs to evaluate its own information systems and apply any given security controls (NIST, 2010a). In this view, security should be considered at all levels of contracting services or when purchasing the software. Thus, this study would reveal the extent to which the government sector uses sound procurement or contracting of security software with a view to achieve robust information security and positive knowledge transfer. Moreover, it would be imperative to examine the extent to which various internal stakeholders in the government sector cooperate and collaborate during the implementation of security measures.

Security of organization information and knowledge can best be managed by planning it in the entire system lifecycle through management support (Swanson, 2001). Even if the lifecycle of IT used in information security may exhibit many models, the main five models that management should focus on are initiation phase, development phase, implementation phase, operation/maintenance phase and the disposal phase (CNSS, 2009). Thus, the ISO through the support of organization management should evaluate potential risks from the initiation to disposal phase. In the context of these phases, this study would only consider the implementation phase, operation/maintenance phase and the disposal phase. This is because the study would assume that majority of security software used in the government sector are outsourced thus eliminating the initiation and development phases.

Disaster recovery also referred to as business continuity planning, forms the last aspect of management controls (Laudon and Laudon, 2004). This process involves creating plans for restoration of communication and computing services after they have been destroyed or disrupted by any event. In this study, two broad classes that would be considered are natural and human-made disruptions. Disaster recovery planning should aim to achieve three goals within information security. The first is to facilitate faster establishment of alternative course of action with regard to processing facility. The second aim is to provide maintenance operations in the alternative course of action. The last aim is to enable the organization to shift production operations back to the initial facility after disaster effects have been resolved (Warman, 1992). Thus, this study will be interested to examine within the study topic how government sector establishes alternative course of action, maintenance operations, and production operations shifts in the presence of either human-made or natural disaster.

## 5.7 Operational Controls

Operational controls refer to those measures that are implemented by human beings and not computer (Casas, 2006). In as much as they can be partly form management controls, they need more technical skills than the majority of management controls. In this category, there are physical security, personnel security and documentation security. Additional elements in this category of controls are incident management and security awareness activities. Therefore, the general argument in this study was that operational controls can be impacted by the management for effective information security program and risk management. The personnel security requires that not all employees should have particular information. On this note, it can be noted that the way people respond to computers and data stored in them is very critical in to the organization. Thus, the management needs to be vigilant on dissatisfying employees who attempt or fall victims of falsifying or tampering with organization data input (Krutz and Vines, 2001). Physical and environmental security requires that an organization take appropriate measures to safeguard systems, supporting infrastructure and buildings against threats that can lead to risks (Freeman, Darr, and Neely 1997). This is due to the fact that loss of transferred knowledge or information can be caused by fire or any other environmental risk.

Poor documentation can pose potential risk management in information security and knowledge transfer. Here, risks of undocumented steps on how a system works, whether technical or non-technical is a key concern that operational controls need to address for effective information and knowledge protection (NIST, 2011b). In this regard, operations manager need to quest for more system documentation that is specific to the organization. Through the help of ISO, should document how information systems work and how they ought to be operated. In this view, security awareness should be adopted as the most recommendable cost-effective approach in reducing risks in information security, knowledge transfer and organization culture shock. Arguably, if employees are aware of threats of certain risks from the social media or social setting then they would devise ways of avoiding them.

### 5.8 Technical Controls

Technical controls require that management of risks, in information security and knowledge transfer, should focus on security controls that can be executed by the computer (NIST, 2006). These controls can provide automated protection against unauthorized use or access, support security requirement for applications and data, and facilitate detection of security violation. Generally, these can be achieved through proper identification and authentication, logical access controls, and audit trails, monitoring and logging (NIST, 2006).

Thus, key issues to be examined in the government sector would be how personnel and systems in charge are used to achieve threat detection, user identification and authentication, logical access controls, audit trails, monitoring and logging. In this regard, this study argued that systems used in government sector should be set to differentiate different levels of users and their access privileges. This process should be based on the nature of classified data as already been discussed in previous chapters. Logical access controls define what should be done, and by who. The system should be set to specify required transactions and functions that are permitted whenever a given level of user accesses the system (NIST, 2006). In this respect, audit trails should be set, in conjunction with other tools, to give information on individual accountability. This allows reconstructing events, identifying problems and detecting intrusions into the system. Hence, the management can use this facility to facilitate investigations in case a major incident occurs to retrieve who used the computer, transaction data and time, and at which terminal was incident incurred. In conclusion, it is required that system log is turned on to its maximum level; a condition that requires installation of logging software into all organization information systems.

## 5.9 Western World view of Information security

The idea of information security takes different views in western world. These differences can be identified in the manner in which national policies treats security around information and knowledge transfer. In Europe, there is strong regulation and enforcement of data privacy. The policy provides individuals the right to respect ones correspondence, family and family life within certain restrictions (Lewis, 2012). In this view, it can be very hard for both government and non-government organizations to know whether an employee is a threat to the organization security due to his/her private background. In another view, the provisions can hamper investigations into information threats especially if individuals' private information is needed to help the organization establish a strong information security. This argument is based on the fact that in Europe, threats to data and information security are not only government but also private companies and the citizens. This suggest that it would be very hard for government organizations to share knowledge with a private sector or citizens especially if it is highly perceived that the act may cause potential risk to the government information.

In every EU state, there is an independent supervisory authority that monitors information and data security (Lewis, 2012). This ensures that government sectors have a superior tier above it to ensure that the expected level of information security is achieved. In contrast, U.S has not legislated data and information privacy and security as Europe (Lewis, 2012). Individual transactions and employment in U.S require that one provides even his/her personal details. However, there is no comprehensive law that regulates how such information should be acquired, stored and used (Lewis, 2012). This poses much threat to employees or stakeholders' information. In another view, government sector can use the strategy to implement strong information security thereby reducing risks in the government sector.

### 5.10 Cultural differences & corporate culture shock

Organization culture shock can shape and can be shaped by organization employees (Ashby, Tommaso and Power, 2012). This is due to the fact that employees may have different backgrounds of organizational, national, and ethnic cultures (Lewis, 2012). Perception can be one element that can contribute to this problem in government sector. Here, majority of English speaking people take themselves as normal, which means that foreigners will be regarded as abnormal. Therefore bringing such people to perform in one government organization may cause much organizational shock due to undermining thought towards others. As a result, the so called foreigners in western world may have the right idea but would intentionally fail to implement the idea.

The element of chauvinism is also attributed to organization cultural shock. This prejudice is highly dominant in western countries especially America. The Americans takes themselves as superior to other nations in regard to their economic, political and social dimensions (Wanning, 1991). The Spaniards think they are the bravest, French think they are intellectually superior, and Japanese think they are just superior in agility. However, Germans admit that they are not as eloquent as French and as big as America though what is quite important is life. This study can suggest that every nation has its prejudice. However, it can be reasoned that employees with different national prejudices can be a potential shock to organizational culture thus needs to be managed. It can further be predicted that the greatest organization cultural shock can occur when western organizations work with non-western organization in which knowledge transfer can as well be hindered.

In view of normality and abnormality as well as perception and assumptions, there are some ethnic and national values that can need to be managed to prevent corporate culture shock. Some countries like Scotland take stubbornness as a positive trait, though in the view of Italians and

English speaking nations, the trait is perceived as intransigence and lack of dexterity respectively (Storti, 1989). Moreover, countries or ethnic groups usually make assumptions on others based on obvious behaviours of the other person. This to some extent can cause corporate shock especially if such assumptions are not correctly interpreted, thereby hindering information security and knowledge transfer. On this basis, this study assumes that every group of nationals has different perceptions on what is normal and abnormal. As a result, this may impact on intra-organisational and inter-organisational information security and knowledge transfer. Thus, the study will analyse how such differences are handled in the government sector in which employees occasionally share information with other employees from another country.

Cultures have been categorized based on national and ethnic lines. Nationally, different nations behave differently thus bringing such varieties under one organization can greatly impact on the management of information security and knowledge transfer. Generally, the Swedes are considered honest, Americans direct, Germans punctual, and Britons true and reliable (Sapir, 1966). Even though it can be noted that the attributes are all positive their applications in achieving potential information security and knowledge transfer can be different.

National cultures can be viewed in two categories: multi-active and linear-active cultures (Hall and Reed, 1983). Hence, this study assumes that government organisations can be conditioned to operate in either of the two cultural dimensions or both. As a result, this can lead to corporate shock. Employees from multi-active cultures are flexible. The culture is acceptable in Portugal and U.S among others but not acceptable in Germany, Britain and Sweden (Hofstede, 1991). These nations accept and practice linear-active culture in which one thing is done at a time within a scheduled time frame. The concept of multi-active and linear-active cultures will therefore be considered in the context of the country of this study to reveal how different views towards time and activity impact on information security and knowledge transfer, and how the public sector has tried to manage it. In as much as national cultural lines can be used to explain how employees from different countries may condition corporate behaviours, it can be argued that there some individuals belonging to such countries but have different cultural behaviours from the national cultures. This implies that this study will not subjectively assume that all employees have similar cultural views and behaviours due to mere fact that they belong to one nation. Thus, a good approach to this issue is to examine how the public sector manages diverse cultural views and behaviours with a view to reduce information risk and increase knowledge transfer among the employees.

In the context of cultural behaviours some cultures value listening but very reactive. Such cultures prefer to initiate an action then listens to the other person. This culture is dominant in the pacific region countries and East Asian countries (Hampden-Turner and Trompenaars, 1993). It can be seen that the culture encourage the concept of *listen before you leap.* As opposed to the western culture, these people would prefer monologue to dialogue. Based on these facts, it can be learnt that corporate shock would arise when employees from two cultures fail to have effective communication. On this note, there are certain instances that effective information security require dialogue and sometimes just require monologue. In another view, some knowledge can best be transferred in dialogue implying that employees from reactive culture would hardly participate in knowledge transfer.

South Europeans are happy when they can perform more things at the same time. This implies that they belong to the multi-active culture (Hofstede, 1980). The only different that these people have with Germans, Americans and Swiss is that they organize their time. Eastern cultures including Indo-Pacific region and Asia view time as a viable alternative. Their time management is not pegged on linear concepts or events to be undertaken but on cyclicality of events (Lewis, 2012). The Eastern cultures peg their behaviours on past events and outcomes. This is quite contrasting to the western culture, which expects Asians to make quick decisions on what to do based on current situation regardless of what happened in the past (Lewis, 2012). Logically, it can be noticed that much corporate shock can occur when a government sector in Eastern countries conducts deals with another government sector in the western countries. In particular, there can be different views on how current information risk and needs or knowledge transfer should be managed to prevent future occurrence of the similar problems. Analytically, it can be seen that Asian corporate can take a longer time to make decisions on security measures on corporate information than western corporate. Similarly, it seems Asian corporate can delay in transferring information from one sector to the other thereby impacting on overall efficiency in risk management.

### 5.11 Managing Risks in Corporate Cultural Shocks

Based on the previous chapter, it can be noticed that transfer of knowledge between the EU-based government organizations and US-based government organization can meet some cultural shock due to their different legal stands in regard to protection of employees' private information. In another view, the transfer of information can be hampered if one nation perceives that the other has not comprehensively implemented information security measures. However, the two nations and their state organizations acknowledge the major principles in information security, which include accuracy, integrity, consent of the subject, as well as the right to review and delete (Lewis, 2012).

The concept of managing risk in organization culture shock has been sparingly addressed across the previous chapters owing to close correlation between the key areas of research in this study. However, this chapter elucidate on this concept further to develop broader understanding. In the context of Milstein (2005), organizational culture entails the beliefs, norms and values that influence the behavior of an organization. In this view, culture describes how things are ought to be done in an organization. Culture can explain why things occur the way they are witnessed. Organizational culture also informs and can be used to define the organization’s risk strategy. Thus, it can be deduced that inconsistency between the expressed risk management strategy and organization culture can lead to difficulty in implementing the risk strategy. In this regard, the management needs to recognize and address the significant influence of culture on risk related decisions (Kirkman, 2010). In effect, this implies that senior management within organizations is key to realizing proper management of risk emanating from culture shocks. The management should further recognize impact of culture shocks from the organisational culture perspective (Kirkman, 2010).

In the organisation-wide implementation of risk management program, the management should ensure that there is a match between employees, processes and culture (Kerr and Slocum, 2005). However, this should be done with new organizational missions, goals and objectives owing to the effect of a new culture in which the organization operates. The risk management strategy as well as communication strategies for sharing risk-associated information should also be revised in a new cultural environment. Therefore, this study argued that effective management of risk that arises from organization culture shock can best be achieved when government organisations incorporate cultural considerations as an essential component in their decision-making processes and strategic-level thinking. Moreover, the author notes that if the organization senior management understands the significance of culture, they would be well placed to achieve organization’s strategic goals regardless of culture shocks (Kerr and Slocum, 2005).

Cultural shock is also evident in situations where two or more organizations merge to operate together. In this regard, there is high likelihood that they would differ in their missions, goals and risk management strategies; willingness to accept risks and propensity to incur risks (Federal Trade Commission, 2005). These culture-related differences can impact on organization performance. Therefore, it can be reasoned that an organization management assesses their partner's perspectives towards risks and business to lay a common ground that would be of befit to both parties in the long-run.

In as much as cultural shocks can be felt across multi-tiered risk management strategy, the senior management is charged with the responsibility to set risk tolerance for the organization. Formally, this can be done through publication of shock management strategy and guidance document. Informally, it can be done through: actions that get penalized and rewarded, consistency in actions, and the degree of accountability shown by an employee (Ashby, Tommaso and Power, 2012). This suggests that employees would try to conform and adjust in the new culture for rewards. On this note, the direction established by senior management as well as their understanding of existing cultural shocks, values and priorities are the key factors that determine how risk is managed (Federal Trade Commission, 2005).

In the context of Federal Trade Commission (2005), there is a strong correlation between risk concepts, trust, and culture shocks. In this view, shifts in organisation missions may call for higher risk acceptance. In the short-term perspective, new measures may be essential to build and establish trust among employees operating in a new organization's cultural environment (Ashby, Tommaso and Power, 2012). In the long-run, such strategies would ensure that the organization employees go well along with evolving organizational norms, values and beliefs. In conclusion, the ultimate goal of managing risk in organization culture shock is to achieve high level of risk acceptance and tolerance.

## 6. RESEARCH QUESTIONS AND OBJECTIVES

Success in the study is based on the nature of research questions used to achieve measurable study objectives. Research questions in the study followed prior mapping and definition of various elements that the study should capture. The following are the specific research questions:

1) What are the different managerial approaches employed in the public sector to overcome the problem of risk in information security, knowledge transfer and corporate culture shock?
2) How does the public sector manages processes, resources and people, as key steps in curbing risk associated with information security, knowledge transfer, and corporate culture shock?
3) What types of risk should be managed in information security, knowledge transfer and corporate culture shock?
4) What are the potential sources of risk that should be managed in information security, knowledge transfer and corporate culture shock?
5) How do different levels of management in the public sector contribute and co-operate towards efficient management of risk in information security, knowledge transfer, and corporate culture shock?
6) How does the public sector manages risks associated with employee transfer and her relations with the private and foreign sectors?

The above lay good foundation for the following objectives:

1) To establish how different managerial approaches are employed in the public sector to manage risk in information security, knowledge transfer and corporate culture shock.
2) To find out how the public sector manages processes, resources and people with a view to curb risk in information security, knowledge transfer, and corporate culture shock.
3) To find out various risk types and risk sources, which should be managed in information security, knowledge transfer and corporate culture shock.
4) To establish how different levels of management in the public sector contribute and co-operate towards efficient management of risk in information security, knowledge transfer, and corporate culture shock.

5) To establish how the public sector manages risks associated with employee transfer and her relations with the private and foreign sectors.

### 6.1 Dividing up Between Doc. 1, 2 & 3

At the beginning, the essence of having a research strategy/plan has been noted.Fisher (2000), Remenyi et al (1998), Gill and Johnson (1997), and Sharp and Howard (199650) advise researchers to have strong research strategy. However, a research is not a linear process (Remenyi et al, 1998), hence the adopted plan must be agreeable to change.

Howard and Sharp's (1996) identify a seven-step model in the process while Remenyi et al model (1998) that identify an eight-step model. Irrespective of the model chosen, the authors emphasise on the significance of topic selection, literature review, concept and theory formulation, conducting the study, completing the analysis, writing up the findings and drawing conclusions. The study will therefore employ these common processes, which are explored in document 2, 3, 4, and 5.

**Document 2**

In the view of Fisher (2000), Remenyi et al. (1998), and Howard and Sharp (1996), an extensive literature review is one of the most significant and preliminary steps within the research process. The review will cover general conceptualization of risk management, components of risk management in information security, knowledge transfer and culture shock, and managing risk in knowledge transfer. Diverse layers of risk management will be explored. The ultimate risk management elements in regard to the information security office staff, security policy, and data classification will be established in the review. Finally, the review will cover different types of management controls geared towards managing the risks.

The literature review will serve as a reference point for the proposed research of *managing risks in information security, knowledge transfer and corporate culture shock in public sector* case study

**Document 3**

The study intends to carry out a sequence of focus groups and in-depth interviews during the course of the study. However, this will be preferred at the outset to explore the concept of on *managing risks in information security, knowledge transfer and corporate culture shock* as it pertains to the public sector. In-depth interviews and focus groups will enable the researcher to identify issues that will be included in the questionnaire. The techniques will also enable the study gather qualitative data to be incorporated in the study.

The study will conduct focus groups and in-depth interviews with:

(i) Managers in different departments within a particular public sector, e.g. Information Technology department, Human Resources department, Planning department, Public Relations departments, Industrial Relations department e.t.c.

(ii) Managers and employees in different job groups/ranks e.g. senior level managers, senior level employees, middle-level managers, middle-level employees, lower-level managers, and lower-level employees.

(iii) Different subgroups, e.g. female employees, male employees, graduates, middle college employees, fresh employees with less than two years in the public sector, and old employees more than five years in the public sector.

Participants will be selected from throughout the organisation while emphasising on different departments, different job groups, and different subgroups. The study proposes also to conduct a series of focus groups with one collection of fresh employees (recruits) since they have not been strongly influenced by the public sector to give wrong views in regard to the subject of study. Nearly ten focus groups and five in-depth interviews will be carried out for the purpose of developing Document 3.

**Document 4**

The researcher will design and administer a questionnaire to a stratified sample of the public sector so as to establish the views of a representative selection of the entire population under study. Stratified sampling involves “dividing the population into mutually exclusive and exhaustive subsets and selecting an independent, simple random sample from each subset (Churchill, 1988:422). The strata that are proposed for this study include (i) job category/rank (ii) role (iii) department (iv) sub-group.

The analysis will focus on frequency breakdown in regard to the study objectives. After the analysis, one will be able to make comparisons of the results with published research on the management of risk in information security, knowledge transfer and corporate culture shock. The research questionnaire will be further improved once the literature review is finished, and the results of the focus groups and interviews are availed.

The researcher proposes to administer the questionnaire in workshop-room situations with various managers and employees from different departments, ministries, and in different job categories. It is expected to have roughly 270 questionnaires completed owing to the size of public employees. The results will be analysed using SPSS software while focusing only on frequency breakdowns.

**Document 5**

The study proposes to use a triangulation approach, based on the content of documents three and four, to develop document five. The researcher will first refine the questionnaire following its initial administration and analysis. The refined questionnaire will then be administered to the selected sample over an eight-month period. Approximately, the study expects to get the views and opinions of 1,000 respondents.

The study will employ four distinct types of analysis on the questionnaire results at this stage. Like the initial survey, the first analysis stage will focus on establishing the frequencies for different variables to note those attributes that exhibit high scores and those with low scores. The second analysis stage will evaluate the variation the respondent’s views and opinions in regard to managing risk in information security, knowledge transfer and corporate culture shock. The third analysis stage will classify various responses into common classes to form themes. The last analysis stage will identify and establish (i) different managerial approaches (ii) various risk types and risk sources (iii) different levels of management. A small number of in–depth interviews (5) and additional focus groups (2) will be carried out to build up qualitative data and to explain any exceptional issues in the study.

# 7. RESEARCH PLAN AND METHODS

## 7.1 Rationale behind Methodology

The question of whether to employ a positivist or phenomenological approach in this study remains to be a major task for the researcher. The researcher proposes to adopt a positivist approach though most authors recommend ethnographic-phenomenological approach for this are of study (Rousseau, 1990; O Reilly *et al,* 1991; Ott, 1989). The problem of selecting the right methodology has been identified by Fisher (2000). Schein (1985) also notes that researcher disagree on how to analyse, measure, understand and manage research data. Moreover, studies suggest a multi-prolonged strategy. Hoftstede *et al*, (1990) recommends the behavioural methodology. The methodology starts with a qualitative perspective and is verified by a quantitative approach. In the multi-pronged research approach, the researcher is required to examine the respondents and their setting through physical observation. The approach also permits the researcher to examine published material, conduct surveys and interviews (Gill and Johnson, 1997). Since every study has its unique strengths and weaknesses, Gill and Johnson (1997) suggest the use of *multi-method*. However, there should be no multiplicity in the use of research approaches. Irrespective of the number of approaches adopted for the study, a researcher should be in a position to justify his/her case and why certain approaches were adopted to prove the case (Remenyi et al, 1998).

## 7.2 Approach for Proposed Study

Based on the established rationale for study methodology, this study proposes to employ the multi-pronged or triangulation research approach as presented by Smircich (1983), Hoftstede and (1990), Claver *et al.* (1999). The approach also fulfils the criteria for the academic programme. In particular, the study will use interviews, focus groups, and questionnaires to collect data. This will take roughly eight months. Data analysis is expected o tae one month then the final month will be used to refine the research report, compile the report, and submit it to the department.

## 8. RESEARCH ETHICAL ISSUES AND ORGANISATIONAL POLITICAL ISSUES

Even though the study proposes to use the members of the public sector to respond to the study, it is acknowledged that there may be falsification of response. However, the researcher is aware of dangers of subjectivity hence this will be avoided at all cost by using strictly what various responses yield.

The researcher acknowledges that trade-offs exist in all studies irrespective of its topic or methodology. The main trade-offs in this study will include the duration and reliability of results. This is due to the fact that the explored topic is not static, but changes relatively with organisational resources, processes and needs.

Even though access to target participants will not be hard, the researcher proposes to seek permission first from the authority to carry out the research. Likewise, the respondents will be required to make informed consent to participate in the study. This implies that the researcher will not force any respondent to participate in the study till the end. The researcher will also not influence how the participants should respond during data collection. This will ensure that the study exhibits high objectivity.

Majority of the interviews and focus-groups will be audio-taped to aid the collection of data. The information that focus groups/interviews will be taped will be explained at the onset of each session and respondents given the liberty to decline to participate or not. The study will ensure maximum anonymity of the participants and this will be assured to all respondents.

# 9. OUTCOME

The proposed study will have significant benefits for the author, the host organisation and the public sector researches in general.

## 9.1 Personal Level

At personal level, the author will have the following benefits:

- Enhance intellectual and academic abilities;
- enhanced perfect research skills and approaches;
- achieve a deeper understanding of a subject that has been of personal interest for a long period;
- use the research experience gained in the real-life work conditions;
- contribute a significant piece of research to the organisation;
- obtain a worthy post graduate qualifications for the efforts applied;

## 9.2 Organisational and Managerial Level

The public sector and its management will benefit by:

- gaining an understanding of a topic that is much referred to but poorly comprehended;
- facilitating future change programmes in the context of risk management;
- having high quality research conducted at no cost to the public sector owing to the author's self-sacrifice on research costs;
- knowing their failures in regard to the study topic and adjust appropriately;
- Objectively knowing how to collaborate with the private and foreign sectors at minimal risk level.

# REFERENCES

Ashby,S., Tommaso, P. and Power, M. (2012). *Risk culture in financial organisations: An interim report* . Centre for Analysis for Risk and Regulation.

Argote L., McEvily B., Reagans R. (2003). *Managing Knowledge in Organizations: An Integrative Framework and Review of Emerging Themes*.

Bayer F., Maier R. (2006). *Knowledge Risks in Inter-Organizational Knowledge Transfer*, Proceedings of I-KNOW 2006 Graz, Austria.

Blebea, N.G. (2011). *Knowledge transfer, ongoing support*, Bucharest.

Banker, R., Datar, S., Kemerer, C. and Zweig, D. (1993). Software complexity and maintenance costs. *Communications of the ACM* V36 (11): 81-94.

Baskerville, R and Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management* V15 (5/6):337-346.

Cummings, J. L. and Teng, B. S (2003). *Transferring R&D knowledge – the key factors affecting knowledge transfer success,* Journal of Engineering and Technology Management.

Casas, V. (2006). *Security Assessment: Case Studies for Implementing the NSA IAM*. Rockland, MA: Syngress Publishing, Inc.

Committee on National Security Systems (CNSS) (2010). Instruction 4009, *National Information Assurance (IA) Glossary*.

Committee on National Security Systems (CNSS) (2009). Instruction 1253, *Security Categorization and Control Selection for National Security Systems*.

Carnegie Mellon University (2005). About CERT. CERT/CC. September 2. http://www.cert.org/meet_cert/meetcertcc.html.

CERT/CC (2001), February 16). *CERT Coordination Center site*. Retrieved February 16, 2004, from http://www.cert.org/present/internet-security-trends/sld016.htm

Claver, E., Llopis, J., Gasco, J., Molina, H., Conca, F. (1999) "Public Administration – From Bureaucratic Culture to Citizen Oriented Culture" in *The International Journal of Public Sector Management.* Vol 12 No5. 1999. pp 455-464

Department of Commerce, United States of America (2004). Federal Information Processing Standards Publication: Standards for Security Categorization of Federal

Egelko, B and Gaura, M. (2003). Libraries post Patriot Act warning: Santa Cruz branches tell patrons that FBI may spy on them. *San Francisco Chronicle*. Available at: http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/03/10/MN14634.DTL.

E-Government Act (2002). *FISMA (P.L. 107-347),* December 2002.

Federal Information Security Management Act (2002). (P.L. 107-347, Title III), December 2002.

Federal Trade Commission (2005). *Privacy Initiatives.* Available at*:* http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Feit, S. (1999). *TCP/IP: Architecture, protocols, and implementation with IPv6*. New York, NY: McGraw-Hill.

Fisher, C (2000) (ed). *Guide to Researching and Writing a Masters Dissertation.* Unpublished handbook for Students at Nottingham Business School.

Gill, J and Johson, P (1997) *Research Methods for Managers.* Paul Chapman Publishing. London.

Harris, S. (2002). *CISSP.* Berkeley, CA: McGraw-Hill/Osborne.

Hofstede, G., Neuijen, B., Daval- Ohayv, D., Sanders G. (1990) "Measuring Organisational Cultures: A Qualitative and Quantitative Study Across Twenty Cases" in *Administrative Science Quarterly,* 35: 286-316.

Hall, E.T. and Reed, H. M. (1983) *Understanding Cultural Differences: Germans, French, and Americans,* Yarmouth, ME: Intercultural Press.

Hampden-Turner, C. and Trompenaars, F. (1993). *The Seven Cultures of Capitalism: Value Systems for Creating Wealth in the United States, Britain, Japan, Germany, France, Sweden and The Netherlands,* New York: Doubleday.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work-Related Values,* Newbury Park, CA: Sage.

Hofstede, G. (1991) *Cultures and Organizations: Software of the Mind, Intercultural Cooperation and Its Importance for Survival,* Maidenhead: McGraw-Hill.

Howard, K., Sharp, JA. (1996) *The Management*

ISACA. (2005). *2006 CISA Exam Bulletin of Information*. Available at: http://www.isaca.org.

ISO_27001 (2005). *Information technology - Security techniques -Information security management systems - Requirements.*

ISO/IEC 15408 (2005). *Common Criteria for Information Technology Security Evaluation*

ISO/IEC 31000 (2008). *Risk management – Principles and guidelines*;

ISO/IEC 31010 (2010). *Risk management – Risk assessment techniques*;

ISO/IEC 27001 (2006). *Information technology – Security techniques – Information security management systems – Requirements*.

ISO/IEC 27005 (2005). *Information technology – Security techniques – Information security risk management systems*.

Kerr, J. and Slocum, J.W. (2005).Managing corporate culture through reward systems. Academy of mManagenet Executives, 5, (19): 43-67.

Kirkman, C. (2010). *Managing culture shock for First Year International students entering Australian universities***.** Helen Cameron, School of Psychology, Social work and Social Policy, University of South Australia. International Services, University of Tasmania

Laudon, K and Laudon, J. (2004). *Management information systems: Managing the digital firm* (8th ed). New Jersey, NJ: Prentice-Hall, Inc.

Lewis, R.D. (2012).When Cultures Collide Leading Across Cultures. *A Major New Edition of the Global Guide.* Boston, London.

Maiwald, E and Sieglein, W. (2002). Security Planning & Disaster Recovery. Berkeley, CA: McGraw-Hill/Osborne.

McCumber, J. (2005). Assessing and Managing Security Risk in IT Systems: A Structured Methodology. New York, NY: Auerbach Publications.

Markus C. Becker, Mette P. Knudsen (2003), *Intra and Inter-Organizational Knowledge Transfer Processes: Identifying the Missing Links,* DRUID Working Paper No. 06-32.

Mitnick, Kevin D. (2002). *The Art of Deception. Indianapolis*, Wiley Publishing, Inc.

Office of Management and Budget (2000). Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

O Reilly, C., Chatman, J., Caldwell, D. (1991) "People and Organisational Culture – A Profile Comparison Approach to Assessing Person Fit". *Academy of Management Journal*. Vol 34. pp 487-516.

National Institute of Standards and Technology (NIST) (2004). Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

National Institute of Standards and Technology (2006). Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*

National Institute of Standards and Technology (NIST) (2006). Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology (NIST) (2011). Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, (Projected Publication Spring 2011).

National Institute of Standards and Technology (2010a). Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

National Institute of Standards and Technology (NIST) (2009). Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

National Institute of Standards and Technology (2011b). Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*.

Pfleeger, C. P. (1997). *Security in Computing.* Upper Saddle River, NJ: Prentice Hall

Roberts, P. (2005). *Malicious Keyloggers Run Rampant on Net. eWeek.com*http://www.eweek.com/article2/0,1895,1893515,00.asp

Remenyi, D., Williams, B., Money, A. and Swartz, E. (1998). *Doing Research in Business and Management.* Sage Publications. London.

Solomon, M and Chapple, M. (2005). Information Security Illuminated. Sudbury, MA: Jones, and Bartlett Publishers.

Schein, E. (1982). Organisational *Culture and Leadership*. 2nd ed. Jossey-Bass. San Francisco.

Schneier, B. (2003). Beyond Fear: Thinking Sensibly About Security in an Uncertain World. New York, NY: Springer-Verlag.

Schneier, B. (2004). Secrets and Lies: Digital Security in a Networked World. New York, NY: Wiley, John & Sons.

Schneier, Bruce. (1999). Security in the Real World: How to Evaluate Security Technology. *Computer Security Journal,* 15:1-14. Available at: http://www.schneier.com/essay-031-ft.txt

Shields, P and Tajalli, H. (2005). The Missing Link in Successful Student Scholarship. Paper presented at the annual conference of the National Association of Schools of Public Affairs and Administration, Washington D. C.

Smiricich, L.(1983) "Studying Organisations as Cultures" in Morgan, G (ed) (1983) *Beyond Method.* Sage. London, 160 –172.

Special Publication 800-37. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;

Special Publication 800-53. *Recommended Security Controls for Federal Information Systems and Organizations*;

Special Publication 800-53A. *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*; and Draft Special Publication 800-30, *Guide for Conducting Risk Assessments*.

Stoneburner, G and Goguen, A and Feringa, A. (2002). Risk Management Guide for Information Technology System. *National Institute of Standards and Technology Special Publication 800-30*. Gaithersburg, MD: National Institute of Standards and Technology.

Swanson, M.. (2001). Security Self Assessment Guide for Information Technology Systems. *National Institute of Standards and Technology Special Publication 800-26*. Gaithersburg, MD: National Institute of Standards and Technology.

Sapir, E. (1966) *Culture, Language and Personality, Selected Essays,* Berkeley and Los Angeles: University of California Press.

Storti, C. (1989) *The Art of Crossing Cultures,* Yarmouth, ME: Intercultural Press.
Tan, Terry (1992) *Culture Shock! Britain,* London: Ernest Benn.

Sveiby K.E. (2000), *La nouvelle richesse des entreprises. Savoir tirer profit des actifs immateriels de sa societe,* Maxima, Paris.

United States General Accounting Office Accounting and Information Management Division. (1999). Federal Information System Controls Audit Manual. Available at: http://www.gao.gov/special.pubs/ai12.19.6.pdf

Updegrove, D. and Gordon, W. (2003). Computer and Network Security in Higher Education: Foreword. *Computers and Network Security in Higher Education*, ed. M. Luker and R. Petersen, x-xxii.avaialbale at: http://www.educause.edu/ir/library/pdf/pub7008a.pdf

Warman, A.R. (1992). Organizational computer security policy. NSE.

Wanning, E. (1991) *Culture Shock! USA,* London: Kuperard.