CHAPTER 2: LITERATURE REVIEW

The literature review was developed through a systematic literature review approach (Biolchini et al., 2005). The literature review is very essential while carrying out any research study. This is because the review of the related literature helps the researcher in understanding the research problem in better way and also helps to find the gap in the researches which have already been done before. By keeping in mind the importance of this, the second chapter of this research has been completely devoted to literature review. In this chapter, views of different studies about the topics related to the present research are critically reviewed.

2.1 E-Government Concepts

E-government concept is to provide government services access over open networks from anywhere at any time. It is considered as the use of ICT in order to communicate with businesses and citizens, and with other government departments (Al-Khouri et al., 2014). With advancements in ICT, e-government is becoming a regular phenomenon and common practice across the globe in the age dominated by the information and communication technologies (ICT) (AlKalbani et al., 2014). With infinite potentials for offering high quality, fast, cost effective government services overcoming the barriers of place and time, the e-government aims to achieve better citizens-government relationship (Taiwo et al., 2012).

2.1.1 E-government- Definitions and Perspectives

E-government can be viewed from different perspectives; such as information systems, computer science, political science and public administration (Heeks & Bailur, 2007).

Seifert and Petersen (2002), identify e-government from two perspectives- political level and technical level. Some identify e-government from a business and technological point of views (Ashaye & Irani, 2012). Tambouris (2001), identifies e-government from four different perspectives: process, citizen, and cooperation and knowledge management. The Table 2.1 summarize some of different e-government definitions:

Table 2.1: Some E-Government Definitions

Author	Definitions
(Abramson & Means, 2001).	Electronic interaction between the government, employees, and the public
("U.S E-Government Act of ", 2002)	Defines e-government as: "The use of web applications and other information technologies by government, combined with processes that implement these technologies, to- *(A) enhance the Government information and services access and delivery to the public, other agencies, and other Government entities; or* *(B) bring Government operations improvements that may include efficiency, effectiveness, service quality, or transformation".*
(UNPAN, 2011)	The use of ICT by government agencies such as Wide Area Networks, mobile computing, and the Internet."
(World Bank, 2009)	"The use of ICT to improve government's (efficiency, effectiveness, transparency, and accountability)."
(OECD, 2003)	"The use of ICT, and particularly the Internet to achieve better government services

2.1.2 E-government Domains

E-government involves various activities in a variety of domains (Almarabeh & AbuAli, 2010). Three e-government interaction domains were identified by the World Bank (2009) which includes government to citizens (G2C) which is the interaction between government and citizens; government to business (G2B) which is the interaction between government and business enterprises, government to government (G2G) that involves different governments' relationship.

2.1.3 E-Government In Developing Countries

As the technology is becoming integral part of every aspect of life, the e-government concept through public administration and organizations across the world is gaining

momentum. E-government uses the tools based on ICT especially web-based application to provide better services to citizens and various types of businesses.

E-government is common in most of the developed and developing countries. However, the rate of e-government adoption in developing countries is slow due to several factors (Rorissa & Demissie, 2010). Some of these factors include: literacy, infrastructure, economic development, and culture. With regards to this view, most of the developing countries share these similarities on political, social and cultural levels. It is important to note here that the gap between the developed and developing countries has increased and is increasing due infrastructure of technologies and the usage of ICT.

E-government invention has been introduced in different ways in developing countries. It embodies design and implementation characteristics of its original context. The inherent properties determine its success while implementing in different contexts (Heeks, 2005; Yonazi, 2010). Therefore, it is imperative to understand and approach e-government with respect to the transfer context. Otherwise, e-government projects may fail because of large difference between design and contextual reality (Maumbe, 2009).

A study by Almarabeh and AbuAli (2010) proposed a general framework for e-government answering various questions such as: What, Why and How of e-government. The study summarizes various factors related to e-government addressing the concept, nature, benefits and challenges in the successful adoption and implementations of e-government projects. However, citizen participation is a very crucial factor for determining the success and failure of e-government. Gebba and Zakaria (2012), have stated that without a guarantee of privacy and security, citizens are unlikely to use e-government services. Therefore, the need to address the concerns of the citizens should be taken seriously for successful adoption and implementation of e-government. Every attempt should be done to establish the balance between privacy concerns of the citizens

and utilizing Internet and other ICT technologies for the betterment of governance and providing fast and maximum comforts and services to the citizens.

2.1.4 E-government in Malaysia

Various countries, including Malaysia, are implementing e-government. The status of e-government implementation is widely discussed in Malaysian context as to the potential of e-government implementation towards the businesses and public. Multimedia Super Corridor (MSC) has been introduced to accelerate Malaysia's entry into Information Age as one of the strategies to achieve Vision 2020. The implementation of e-government was initiated by the introduction of the MSC in 1996 in Malaysia (Ramli, 2012).

However, e-government implementation in Malaysia is facing many challenges. Of the challenges, the technological challenge is the main challenge which includes issues like standards, legacy maintenance, data integration, and privacy and security (Kaur et al., 2014). To improve the core government applications and integrating more services across agencies is the key priority in Malaysia (Kaur et al., 2012). In General, the new technologies are forcing governments to be particularly attentive to time. To keep pace with the fast moving world of the technology, government of Malaysia need to provide a quality e-government services to enhance confidence among citizens to use the online services provided by government in more efficient and effective way. In short, implementing good strategies must be addressed carefully. Otherwise, e-government will remain a misleading, cosmetic operation (Lean et al., 2009).

2.1.4.1 Public Service Department Malaysia (JPA)

The administrative arm of Malaysian government is the Public Service Department Malaysia (JPA). It has a crucial role to play in facilitating the nation's journey towards becoming a developed nation by 2020. The government has already put in place

comprehensive transformation agenda encompassing the government, economic, political and social transformation Program.

The objectives of JPA are:

- To rationalize the size of public service through a systematic and structured human resource planning, and provide the public service with service schemes and organizational structure.
- To develop the best and competent human capital to meet the public service's strategic needs through dynamic training programs
- To formulate and implement an effective service policies, and enhance the quality of service delivery.

Therefore it is selected for data collection as participants for the questionnaire data.

2.1.5 E-government Development Models

E-government development models (eGDMs) describe the different e-government development process until it reaches its highest potential stage. Some books have treated e-government implementation and development process into different phases. One phase does not need another to be completed for another to begin. (Al-Hashmi & Darem, 2008). In this section following models were investigated and analyzed for the level of available security services which are summarized in the following Table 2.2.

Literature reviews of different eGDMs have shown that there is a lack of socio-technical and technical security requirements eGDMs stages. Therefore, there is a need to focus upon these issues into eGDMs stages.

Table 2.2: E-Government Development Models Concept.

The Model	The Model Stages	The Model Proposed
(Moon, 2002).	**Five stages:** Simple information dissemination (one way communication), Two-way communication (request and response), Service and financial transactions, Vertical and horizontal integration, and Political participation.	Focuses on functionality, potential benefit of e-democracy
(Siau & Long, 2005)	**Four stages:** Interaction, Transaction, Transformation, and E-democracy	Focuses on Citizen-centric and potential benefit of e-democracy
(Layne & Lee, 2001)	**Four stages:** Catalogue, transaction, vertical integration, and horizontal integration.	Developed based on technical, managerial and organizational feasibility
(West, 2004).	**Four stages:** Billboard, the partial service-delivery, the portal with fully executable and integrated service delivery, and Interactive democracy.	Focuses on functionality and citizen-centric
(Deloitte &Touche, 2001).	**Six stages:** Information publishing, two-way transactions, Multi-purpose portals, Portal personalization, Clustering of common services, and Full integration and enterprise transformation.	Focuses on citizen-centric
(Howard, 2001).	**Three stages:** Publishing, Interacting, and Transacting.	Focuses on functionality and citizen-centric
(Hiller & Belanger, 2001)	**Five-stage:** Information, Two-way communication, Transaction, Integration stage, and Participation.	Focuses on functionality, potential benefit of e-democracy

2.1.6 E-Government Security Frameworks

E-government security frameworks guides and facilitates government organizations to offer an effective e-government security services. Information security must be carefully considered as a serious requirement of securing e-government services. Six e-government security frameworks are reviewed in this section.

- Kessler et al. (2011) proposed framework which aimed to analyze the necessary requirements for privacy as a success factor in e-government systems. The framework identifies major issues related to the privacy in citizen-oriented e-government systems.
- Belanger and Hiller (2006) developed a framework that identified e-government privacy issues- analyze the global motivators and constraints effect, and facilitate decision-making. This is an important process to evaluate in depth complex issues, such as e-government privacy.
- S. M. Alfawaz (2011) proposed a managerial e-government security framework for developing countries. It addressed related variables from different perspectives such as security, cultural, organizational and managerial.
- Al-Ahmad and Al-Kaabi (2008) proposed an enhanced e-government security framework. The framework considered the people, processes and technologies aspects of e-government security.
- Setiadi et al. (2013) proposed a Balanced e-Government Security Framework. This framework contained multi-layer components including-asset layer, requirement layer, protection layer and the success factors of information security implementation. The protection layer described e-government security control. This layer includes components such as administrative security, logical security and physical security.
- Chetty and Coetzee (2010) proposed a Service-oriented Architecture (SOA) security framework. The framework consisted a variety of controls that can minimize the information security challenges. These controls collectively provided direction for management, strategic, operational and technical levels to implement SOA information security.

The review of these frameworks showed that these frameworks missed rest of the security control principles and best practices elements which are related to people and processes components of information security management. This leads to the need to focus on the socio-technical approach to match the pertinent security requirements into the e-government implementation.

2.2 Information Security- Overview And Concept

Information security is defined as the protection of information from threats to minimize business risk accordingly to ensure business continuity (Mvungi & Makoko, 2012). The rise of e-government has been one of the most striking to web based applications developments. It requires a great deal information about security more than just a solid website that provides the right content (Upadhyaya et al., 2013). E-government today must deal with the risks of information security due to various reasons. The success of e-government project requires facing all the challenges addressed in implementing e-government, especially the security challenge. According to Singh and Karaulia (2011) the basic security concepts are:

- **Confidentiality:** assures that private information is protected and kept safe from unauthorized individuals.
- **Integrity:** is about protecting information from being modified by unauthorized parties.
- **Availability:** is to ensuring that systems work and services are provided promptly to those who are authorized to use them.

These concepts are important to information on the Internet which contributes to making the e-government environment a secure and safe environment.

As mentioned earlier, e-government refers to the using of information technology to build up a virtual e-government and break the boundary of administrative organizations. However, such organizations are facing a wide range of information threats. Therefore, information security is the most important factor in their information systems and therefore must be carefully considered and presented in all of development stages as an element, from requirement analysis to implementation and maintenance (Al-Khouri et al., 2014; Singh & Karaulia, 2011). In other words, information security has become critical issues of fundamental importance in our society (Wang, 2009). Without the assurance of

security, citizens are unlikely to use e-government services. Therefore an increased variety of security services is required (Rose & Grant, 2010; Wangwe, 2012).

2.2.1 Security standards

While security is an important factor to protect the organization data, there is a need for a standards or guideline to ensure that an adequate level of security is attained. Generally, the best security practices are adopted, and resources are used efficiently (HKSAR, 2008). Thus, the purpose of standards is to assure the confidentiality, integrity and availability of organization information (ISO, 2005).

2.2.1.1 ISO standards

ISO standards are issued by the International Organization for Standardization (ISO) which covers many areas such as IT and its security management systems. It was designed to help the organizations in managing their information security effectively (ISO, 2005). ISO/IEC 27002:2005 is code of practice for information security management (Suduc et al., 2010). ISO/IEC 27002 contains 12 major domains such as asset management, security policy, human resources security, physical and environmental security, organization of information security, communications and operations management, information systems acquisition, access control, security incident management, compliance, business continuity management, risk assessment (ISO, 2005; Von Solms & Van Niekerk, 2013).

2.2.1.2 COBIT Standard

Information Systems Audit and Control Association & Foundation developed The Control Objectives for Information and related Technology (COBIT)(ISACA, 2012). COBIT Standard provides framework for information technology (IT) management and business process and IT governance to help understand and manage the risks associated with IT. (ITGI, 2013). COBIT describes the need of the processes and controls for implementing an information security policy. It contains a brief section on Security and

Internal Control Framework Policy, which gives various pointers on writing and maintaining such a document. Plan and organize, acquire and implement, deliver and support, and monitor and evaluate are the four main components of COBIT (Z. Ismail et al., 2010).

2.2.1.3 ITIL Standard

The Information Technology Infrastructure Library (ITIL) was developed in 2005 by the United Kingdom's Office of Government Commerce (OGC) ("Best Management Practice," 2007). It is a set practice for IT service management (ITSM). It focuses on aligning IT services with the needs of business and considers the central role of the user (Mesquida et al., 2012). ITIL describes processes, tasks, procedures, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It is used to demonstrate compliance and to measure improvement.

2.3 The Socio-Technical Approach

Socio-technical systems theory has been used for decades as a framework to design and understand organizations, and has been applied in practice as a framework for organizational change.

2.3.1 Socio-Technical Model (STM)

Socio-Technical Model (STM) was developed by S. Kowalski (1994) as presented in Figure 2.1. The model is divided into two sub-systems such as social (culture and structures) and technical (methods and machines). He argues that every system strives to be in balance. So when any of the components or subsystems changes, then other components change too, to keep the balance.

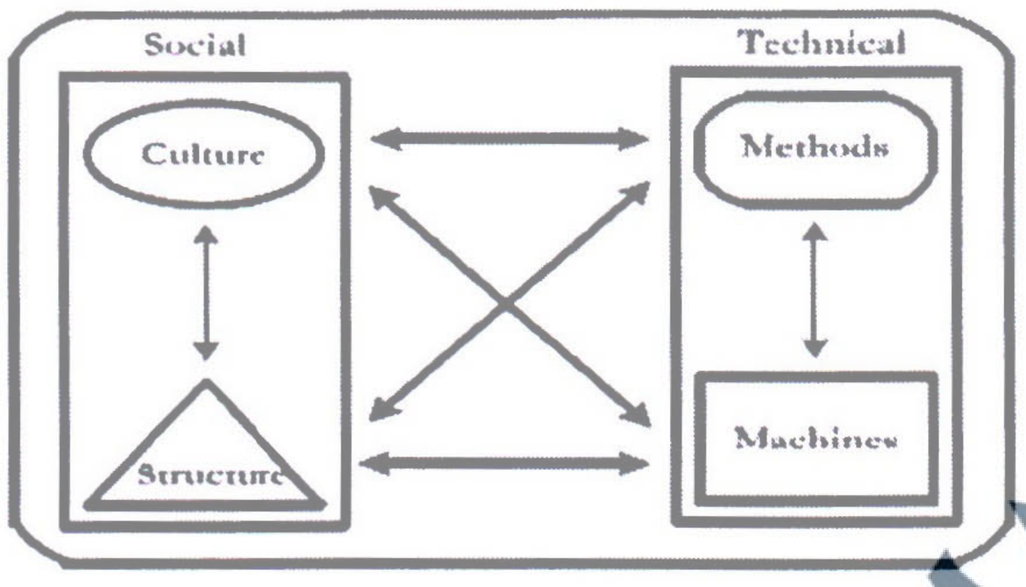

Figure 2.1: Socio-Technical Model (Kowalski, 1994)

2.3.2 Security By Consensus (SBC) Model

Security-By-Consensus (SBC) was proposed by (S. Kowalski, 1994). SBC model showed detailed part of socio-technical model that reflected how security could be modeled as is shown in Figure 2.2. It consist two sub-systems such as social sub-systems which includes (ethical and cultural, legal and contractual documents, administrational and managerial policies, and operational and procedural guidelines) and technical sub-systems which includes (mechanical and electronic, hardware, operating systems, application systems, and data). Other aspects are: store, process, collect, and communication.

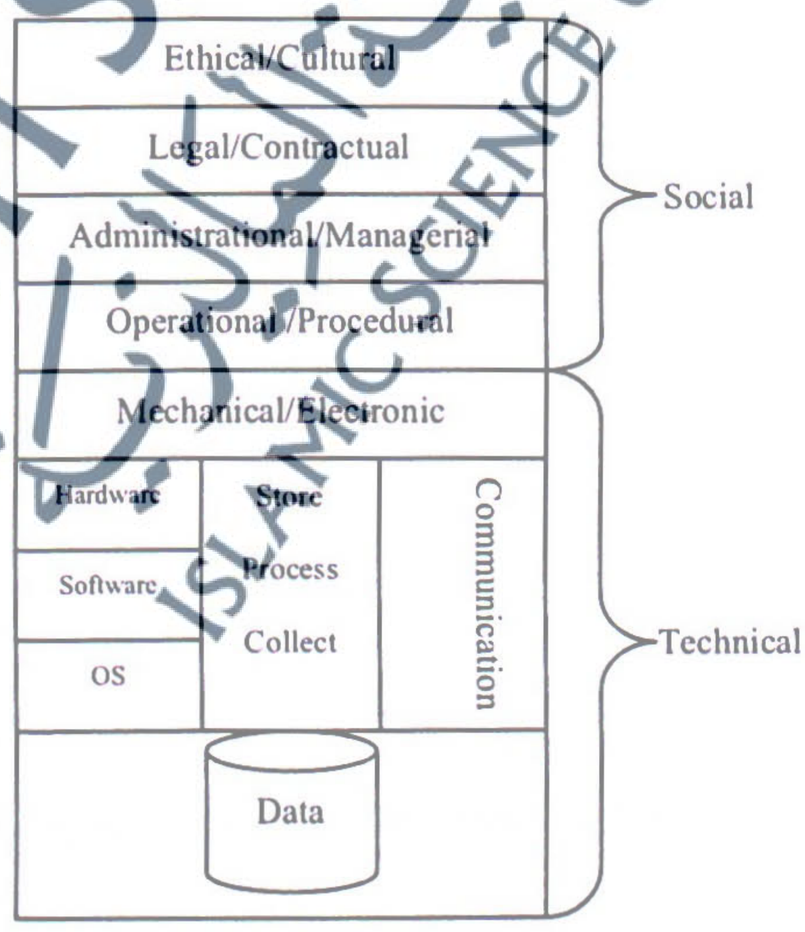

Figure 2.2: The basic SBC Model (Kowalski 1994)

Tarimo (2006) developed a mapping of ISO 27002 security management controls with SBC model basis, which is considered as themes in this study as shown in Figure 2.3. This helps to easily comprehend security controls and issues at organizational level under study (Tarimo, 2006). This research used Tarimo mapping as tools to guide the analysis criteria to analyze each model and framework for the level of available security controls.

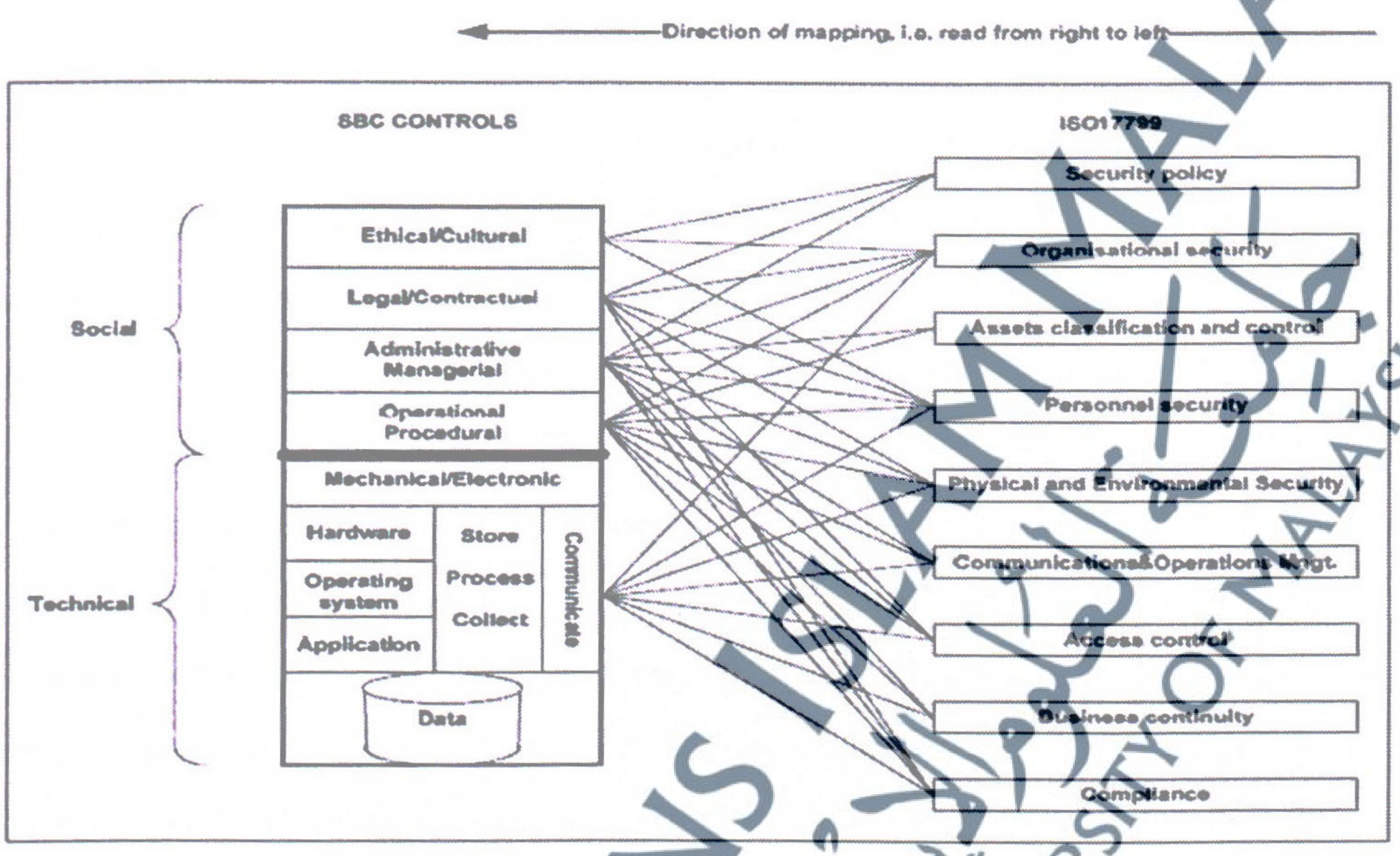

Figure 2.3: Mapping the Desired ICT Security Management State (ISO 17799) onto the SBC Model (Tarimo, 2006)

2.4 Information Security Culture

Information security culture research is still in early stages of development (M. A. Alnatheer, 2015; Ramachandran et al., 2008). Along with the growing interest in this field, there seems to be hesitance and little agreement within the literature as to what information security culture actually is (Ramachandran et al., 2013). Information security culture can be defined as "all socio-cultural measures that support technical activity methods, so that information security becomes a natural aspect in the daily activity of every employee" (Schlienger & Teufel, 2002), . While, Ngo et al. (2005) defined it as "how things are done by employees and the organization as a whole (i.e. accepted behavior and actions), in relation to information security". Da Veiga and Eloff (2010) defined the Information Security Culture as the "attitudes, beliefs, assumptions, values

and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time". Information security culture is the assumptions of which types of information security behavior are accepted and encouraged by the employees of the organization (Lim et al., 2010).

According to UK Government Report, only 5% of all the data loss in the UK is because of technology related issues whereas 95% of it, is by due to cultural related factors of people (Colwill, 2009). Therefore, researchers have stated that to achieve an adequate level of securing the organizations information, the information security culture must be concerned as important factor, and must gain more attention (Brady, 2011). D'Arcy and Greene (2009) argued that a significant change in security culture can reduce the number of security breaches experienced. However, it is necessary to establish a security culture as the key to manage human factors in all organizations (Metalidou et al., 2014; JF Van Niekerk & Von Solms, 2010). Therefore, to achieve this aim, security managers need to take time to understand the cultural construct regarding the implementation of security effectiveness of information systems in organizations (Flores et al., 2014).

Study by AlHogail and Mirza (2014) concluded that, 62 papers, published in the period of 2003–2013, focused on information security culture in organizations. Only 22% of the total number of papers (14 papers) presented a framework. The frameworks discussed different specific issues, and few touched on human components such as awareness and training. However, most of the available frameworks lacked a comprehensive view that integrated humans, organizations, and technology to provide organizations with an all-inclusive framework to aid organizations' information security practitioner in the implementation of an information security culture.

2.5 Information System Security Effectiveness

Measuring the effectiveness of security in information systems is an issue that has seriously been questioned among academics and practitioners (Mishra & Chasalow, 2014). The effectiveness of security measures in reducing the overall risk to information in organizations had been studied extensively over the years (S. Alfawaz et al., 2008). Radack (2008) argued that the security controls such as the management, operational, and technical safeguards or countermeasures that protect the confidentiality, integrity, and availability of an information system and its information, effective information security in organizations depends on these controls (Aliti & Akkaya, 2011).

2.5.1 Information Security Effectiveness Models And Frameworks

- **Straub model**

One of the first models on Information System security effectiveness has been provided by Straub Jr (1990). The model was based on the General Deterrence theory (GDT) which investigated whether a management decision in Information System security is more effective control of computer abuse. He argued that security countermeasures that include preventive security software and deterrent administrative procedures would result in lower computer abuse.

- **Kankanhalli model**

Kankanhalli et al. (2003) proposed a conceptual model of information system security effectiveness. Their theoretical model included organizational factors such as Top management support, Organizational size, and Industry type. They also found that Information System security effectiveness could increase by greater preventive measures and deterrent efforts.

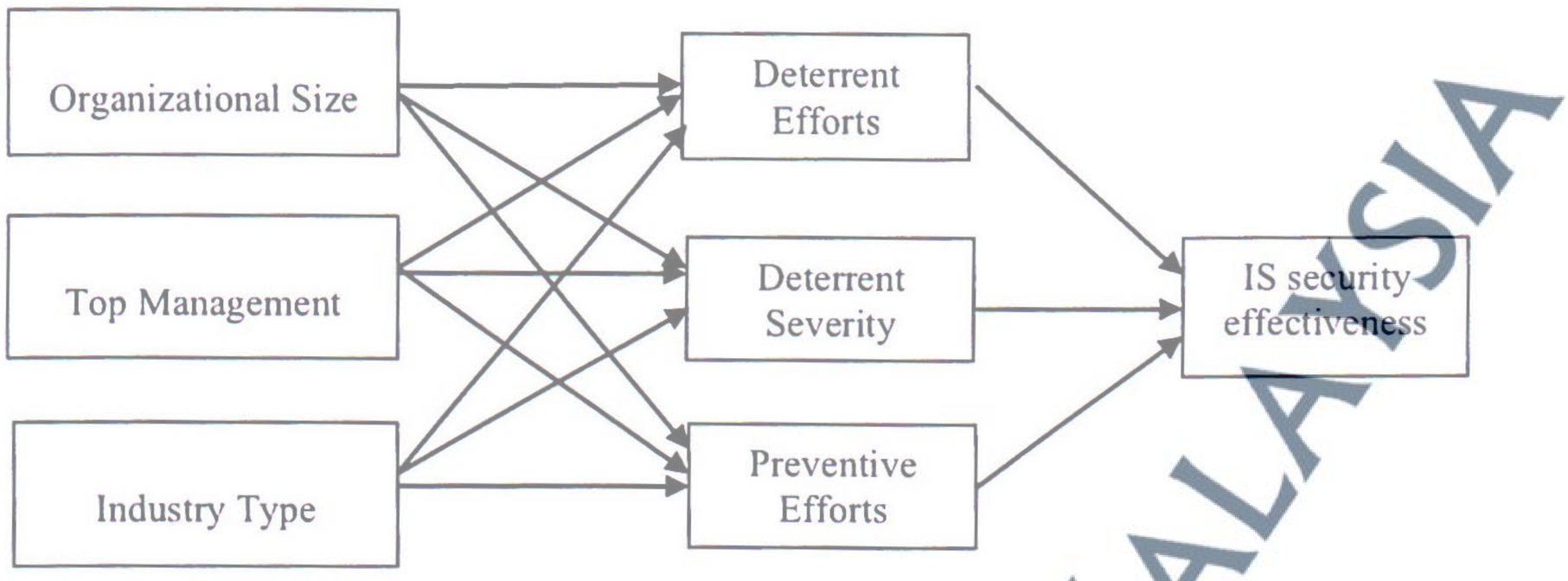

Figure 2.4: Model of IS security effectiveness (Kankanhalli et al., 2003)

- **D'Arcy and Hovav model**

D'Arcy and Hovav (2009) used the term ''security countermeasures'' to describe technical and procedural controls. By use of an extended deterrence theory model, certain controls for Information System misuse were identified. The results of their study mentioned that three practices deter Information System misuse such as security policies, education, training, and awareness programs; and computer monitoring. The result showed that security awareness is the most countermeasures against human factor in threats to information security.

- **Da Veigaand Eloff framework**

Da Veiga and Eloff (2010) focused on employee behavior and have investigated security effectiveness in terms of security culture by presenting a framework to develop an information security culture in an organization.

- **Herathand Rao framework**

Herath and Rao (2009) stated that both intrinsic and extrinsic motivators can influence security behaviors of users. They assessed the effectiveness of the security model consisting of various motivating factors such as penalties, pressures and perceived

contribution that encourages information security behaviors in organizations. The study mentioned that creating a general culture that fosters security is a better strategy in information security.

- **Brady framework**

Brady (2011) suggested a theoretical HIPAA security compliance model in U.S.A academic medical centers. The model is based on socio-technical factors such as awareness, culture, management support, and computer self-efficacy. The results showed that these factors were important predictors of security effectiveness and security behavior.

- **Ayyagari &Tyks framework**

Ayyagari and Tyks (2012) addressed the data breaches that are caused by lax security policies and included an element of social engineering. The results showed that Top Management Support, Policies, and Awareness at the university improved security effectiveness. Thus, literature review of different security models and frameworks have emphasized that through implementing all the required information security components, organizations must govern information security effectively (Brady, 2011; Da Veiga & Eloff, 2010; Herath & Rao, 2009; Veiga & Eloff, 2007).

2.6 Socio-Technical Factors

Information security management has become an important issue these days. Lee et al. (2004) have stated that enhancement of social bonds through organizational factors is an effective mechanism in preventing computer abuse. Though some of the information security research has considered organizational issues or socio-technical issues, it has primarily focused on technical issues concerning the design and implementation of security subsystems (Choo, 2011; Crossler et al., 2013). However, it should be noted that

information security could include technical and socio-technical aspects. Real information security governance therefore consists of ensuring that both these technical as well as the non-technical aspects are implemented and coordinated in a holistic way (H. Chen & Li, 2014).

Many studies have focused on the information protection issue mostly from technical perspective (D'Arcy & Hovav, 2009; Shaaban, 2014). However, information security, related to socio-technical aspects, need to gains more attention. Organizations need to realize that the information protection is a business issue and not a technical (Dzazali & Hussein Zolait, 2012; El-Haddadeh et al., 2012). These studies concluded that organizations focus solely on the technology itself and neglect the people, processes and business goals that support the technology. However, the realization that social factors pose greatest information security threat to an organization which needs to be addressed (J. H. Hall et al., 2011). Other studies have concluded that a socio-technical approach is necessary for holistic addressing of information security. Information security management would not be complete without the social factors consideration besides the technical factors (Kayworth & Whitten, 2010; Loser et al., 2011; Shaaban, 2014; Wangwe, 2012). To address the literature gap, the impact of technical and social factors have to be given more attention in encouraging positive information security culture (Narain Singh et al., 2014).The majority of the above mentioned studies have concluded that the socio-technical aspect is as important as technical aspect for implementing an effective information security program.

Table 2.3 provides socio-technical factors that influence information security effectiveness. As illustrated in Table 2.3, there are many factors found to be important elements of information security. However because of the scope limitation, the current study will only consider the top constructs where there is strong agreement between academic researchers as to their importance for security culture creation. The current study extracted the top nine constructs as candidate constructs and constructs of interest

for the conceptual model. These factors are: Legal & law, Compliance, Ethical Conduct, Security culture, Security Policy, Security Awareness, Security Training, Top Management Support, IS structure

Table 2.3: Socio-Technical Factors Influence Information Security

Factors	Number of Times Cited out of 20 studies	Factors Rankings
Top Management Support	16/20	1
Security Policy	15/20	2
Security Awareness	14/20	3
Security Training	14/20	4
Security culture	13/20	5
Compliance	13/20	6
Ethical Conduct	13/20	7
Legal & law	11/20	8
IS structure	10/20	9
Assess management	7/20	10
Change management	6/20	11
Risk assessment	6/20	12
Trust	4/20	13
Integrity	3/20	14

2.6.1 Successful Socio-Technical Factors

This section explores the success of socio-technical factors which are related to information security which influences e-government security. It is reported that information security incidents are increasing even as organizations invest more in technical solutions (Symantec, 2009). More recently researchers have started to realize that technological factors are not the only key to achieve an effective information security. Human and organizational factors' impact need to be taken into consideration as well (Furnell et al., 2009; Herath & Rao, 2009). The understanding of how different technological, human, and organizational elements interplay could explain how different factors lead to secure the organizations (Knapp et al., 2009; Kraemer et al., 2009).

However, organizations need to invest in both technical and socio-technical resources to achieve success in information security (M. A. Alnatheer, 2014; Chang & Ho, 2006).

Various studies have stated that information security policies have effective influence on information security (S. M. Alfawaz, 2011; Knapp et al., 2009). Some studies have linked the effect of organizational culture on information security policy and managerial effectiveness (Knapp & Ferrante, 2014). The most important control to protect organizational information from threats is information security policy (M. Siponen et al., 2014). Many incidents of information security are caused by human behavior (Beautement et al., 2009). This demonstrates a negligence or ignorance of the organization security policies. Employees often do not understand enough about the impact of their security decisions and are not aware of the security consequences of their actions (D'Arcy et al., 2009; M. Siponen et al., 2010). This can be resolved if a clear vision from senior management is presented to influence employees' behavior to protect the organization's information assets through compliance with the security policy (M. Siponen et al., 2010). The security culture of the organization will improve through the compliance with security policy (M. A. Alnatheer, 2014; Hassan & Ismail, 2012). Ruighaver et al. (2007) have argued that effectiveness of organizational security does not start with anti-virus or firewalls software, but with top management support, training and awareness programs could influence the culture of an organization (Knapp & Ferrante, 2014). Top management support is important factor for information security effectiveness (Knapp & Ferrante, 2014; Kraemer et al., 2009), and information security awareness is critical factor of information security management (Hu et al., 2012; M. T. Siponen & Oinas-Kukkonen, 2007). Training and awareness factors are some of the most effective countermeasures against the human factor threats to information security (Parsons et al., 2010).

Researchers have argued that creating a security culture within organization settings is necessary and important for effective information security management (S. M. Alfawaz,

2011; Da Veiga & Eloff, 2010). Shahri et al. (2013) argued that the security culture, security training and awareness help to implement an information security effectively. Information security is primarily a management problem and how management deals with information security is a direct reflection of an organization's culture (Ruighaver et al., 2007). Security culture have a strong impact on the organizations security (Parsons et al., 2010). Many studies have concluded that information security culture establishment is necessary and important for effective information security management (S. M. Alfawaz, 2011; Da Veiga & Eloff, 2010; Flores et al., 2014).

Several studies have also argued that information system structure is important for effectiveness of any information system project. It is an important factor that could influence information security effectiveness (S. M. Alfawaz, 2011; Hussein et al., 2007; Ma et al., 2008). Thus information system structure has been identified as important factor that could lead to success of information security implementation in the electronic government setting (Hussein et al., 2007).

The broad existing research has recognized different issues and challenges in developing countries which include- gap between technology and cultures (Heeks, 2003), lack of adequate infrastructure and lack of legal development, (Abu-Musa, 2010; Knapp et al., 2009). The information security management system (ISMS) includes many aspects such as standards, guidelines, policies, technology, legal and ethical issues, and human issues. There are number of diverse factors need to be considered while setting e-business security management and policy such as organizational, administrative, technical, legal and human issues. The ethical and operational security measures could be affected by the legal security measures, which could necessitate a change in the current ethical controls (Mwakalinga, 2011). The security behavior of organizational members should be improved by the measures of cultural and ethical issues (M. A. Alnatheer, 2012; M. Siponen & Vance, 2010). Ethical conduct helps to ensure that employees are adhering to the security policy. Therefore, the protection of information should be based on the

organization's information security policies and ethical conduct (Al-Omari et al., 2013; Ruighaver et al., 2010). Thus, in addressing security problems, the ethical conduct plays a major role. Therefore, it must clearly state which actions are ethical and which are not (S. Alfawaz et al., 2008). The ethical conduct has not been investigated in most information security frameworks (Flowerday & Von Solms, 2006; Veiga & Eloff, 2007).

Table 2.4: Successful Socio-Technical Factors.

Constructs	Factors	Reference
Legal/ Contractual	Legal & law	(Da Veiga & Eloff, 2010), (Hwang et al., 2004), (Wang, 2009),(Al-Tameem et al., 2009), (Hagen et al., 2008), (AlKalbani et al., 2014)
	Compliance	(Schlienger & Teufel, 2005), (Ramachandran et al., 2008), (Tarimo et al., 2006), (M. A. Alnatheer, 2014)
Ethical/Cultural	Ethical Conduct	(Da Veiga & Eloff, 2010), (Dojkovski et al., 2007), (Tarimo et al., 2006), (Al-Salihy et al., 2003)
	Security culture	(Dojkovski et al., 2007), (M. A. Alnatheer, 2014; Knapp & Ferrante, 2014), (Hassan & Ismail, 2012), (Brady, 2011), (Kazemi et al., 2012), (Knapp et al., 2007), (Hagen et al., 2008), (Robbins & Judge, 2012),
Operational /Procedural	Security Policy	(Da Veiga & Eloff, 2010), (M. A. Alnatheer, 2014), (Schlienger & Teufel, 2005), (Dojkovski et al., 2007), (Tarimo et al., 2006), (El-Haddadeh et al., 2012)
	Security Awareness	(Ramachandran et al., 2008), (Ayyagari & Tyks, 2012), (El-Haddadeh et al., 2012), (Hassan & Ismail, 2012), (Knapp & Ferrante, 2014), (Al-Tameem et al., 2009)
	Security Training	(Knapp & Ferrante, 2014; Schlienger & Teufel, 2005), (Dojkovski et al., 2007), (Kraemer & Carayon, 2005), (Tarimo et al., 2006), (Ayyagari & Tyks, 2012)
Administrative /Managerial	Top Management Support	(Johan Van Niekerk & von Solms, 2006), (Ayyagari & Tyks, 2012), (El-Haddadeh et al., 2012), (Kankanhalli et al., 2003)
IS structure		(S. M. Alfawaz, 2011), (Hwang et al., 2004), (Al-Tameem et al., 2009), (Hussein et al., 2007)
Security Effectiveness		(Knapp & Ferrante, 2014), (Mishra & Chasalow, 2014), (Kankanhalli et al., 2003), (Brady, 2011).

Based upon review of previous and current approaches towards e- government security, and by putting together the literature on security effectiveness, successful socio-technical factors have been identified in Table 2.4, and next sections discusses these factors in detail.

2.6.1.1 Legal and law

Legal factors play a major role in addressing information security problems. Lack of legal development is one of the information security challenges in an organization (S. M. Alfawaz, 2011). Legal factor has the potential of becoming a failure point of information security implementation. It could affect the information security in organization. Therefore, it needs to be a properly addressed (Mwakalinga, 2011). In addition, if an employee commits fraud, there must be a legal framework that addresses information security related cases. Prosecuting people who commit illegal actions will not be effective if such a framework is lacking (Hagen et al., 2008).

Information security measures avoid violations of legal requirements. Efforts must be made to meet legal requirements which in turn should prevent possible security breaches (Breaux & Baumer, 2011). In this respect, effectiveness is understood as the ability of a measure to assist the organization to meet legal requirements (Hagen et al., 2008). Thus, legal aspect is one of the critical factor which need to be considered in information security management (Olusegun & Ithnin, 2013). Al-Tameem et al. (2009) stated that the organizational, technical and legal are three critical factors that impact the implementation of information security. As legal aspect is considered as one of the important factors that could influence the information security effectiveness, it would be a candidate factor for the research conceptual framework.

2.6.1.2 Compliance

As complying with security policies leads to effective information security management and security culture, many organizations found this a major challenge while trying to influence security behavior of the employees to comply with information security policy (Beautement et al., 2009). It is estimated that over half of all information system security breaches are indirectly or directly caused by employees' poor Information System security compliance (M. Siponen & Vance, 2010). Therefore, there is a need to find a

method to ensure the compliant behavior of employees and to measure the compliance program effectiveness. Researchers have suggested that organizations can influence the behavior of employees by cultivating a security culture that promotes security-conscious decision-making by complying with the information security policy (D'Arcy & Greene, 2009). Da Veiga (2015) indicated that there is a strong relationship between compliance, culture, and employees' behaviors. This shows that the complying with information security policy is important for the establishment of security culture and improves the security effectiveness in organizations. This is important because the security culture goal is to influence the employees' behavior with respect to complying with the information security policy (D'Arcy & Greene, 2009). Based on the previous discussion, it can be asserted that security compliance is an important factor for security culture establishment and it is considered as a candidate factor for the research conceptual framework.

2.6.1.3 Ethical Conduct

Ethics can be defined as, "The values and rules that distinguish right from wrong" (Hellriegel et al., 1998). Ethical conduct "facilitate responsible security awareness, as users are held personally responsible for ensuring sound security practices which are implemented, reducing the security risks" (Mears & von Solms, 2004). It is important to integrate ethical behavior relating to information security into employees' everyday life in the organization (Al-Omari et al., 2013).

Information security ethics is an important factor for addressing security problems. It is one of the principles in creating a security culture (C. C. Chen et al., 2008). In addition, ethical standards and policies can differ between countries (Dojkovski et al., 2007). Ethical conduct has been ignored in previous research of information security culture with one exception which pointed out that those different nations and companies that have their own cultures of companies sharing relevant knowledge, can strengthen information security culture (Helokunnas & Kuusisto, 2003). This shows a gap which is the investigation of the importance of ethical conduct policies for security culture creation

that needs to be addressed by academic researchers in the information security field. Therefore, ethical conduct will be a candidate factor for the research conceptual framework.

2.6.1.4 Information Security Policy

The organization information security policies deal with "the procedures and processes that the employee should adhere to protect the confidentiality, integrity and availability of information" (Knapp et al., 2009). The information security policy purpose is "to create a shared vision and an understanding of how various controls will be used such that the organization data and information is protected" (Dhillon et al., 2007). The security policy can enhance the effectiveness of an information security management (Herath & Rao, 2009). Organizations cannot achieve effective information security management without the establishment of an information security policy (Al-Awadi & Renaud, 2007; M. A. Alnatheer, 2012).

Security policies are extremely important not only for information security management effectiveness, but also to cultivate an information security culture in an organization (M. A. Alnatheer, 2014). This shows that having an effective information security policy is important for creation of a security culture and the improvement of an organization's security effectiveness. Based on this review, the current study concluded that establishing an effective information security policy has a strong influence on the creation of a security culture. Therefore, it has been included as a candidate factor for the research conceptual framework.

2.6.1.5 Security Awareness

Information security awareness is one of the important factors that could have impact on information security management (Hu et al., 2012). It is the top obstacle to information security (S. Alfawaz et al., 2010).

In some cases, security awareness is only concentrated around the IT department and does not include employees in the organization. This is a major problem if organizations do not realize the importance of having security awareness amongst employees (M. Alnatheer & Nelson, 2009). Information security awareness levels are still found to be low among the employees of organizations and organizations are nevertheless still not making any effort to implement awareness programs to improve the situation (Koskosas et al., 2011). Therefore, it is important to establish an information security awareness program for securing information technology environment (ISO, 2005). The organization should implement the security awareness program at all levels, from top management to down to every employee (ISO, 2005). The importance of security awareness has been highlighted in previous discussions as a vital part of information security protection and creating an effective approach to manage information security. However, security awareness is an important factor for creating security culture (Akhgar & Arabnia, 2013; Chan & Mubarak, 2012). Security culture can be improved by increasing the awareness of users. Therefore, top management must take seriously security awareness to ensure not only information security effectiveness but also to improve the security culture. Based on this discussion, security awareness has strong influence on the creation of a security culture and has been included as a candidate factor for the research conceptual framework.

2.6.1.6 Information Security Training

M. A. Alnatheer (2015) argued that security training should be provided to improve security awareness. It has been argued that proper education and security training help change people's behaviors toward security. People will always be the weakest link and the organization will still be at risk without security awareness and training programs (Wipawayangkool, 2009). To improve security awareness, the security training is required for all employees. It is important for the creation of an information security culture (Crossler et al., 2013). Organizations need to ensure that "training, education and awareness will improve the information security culture, and minimize risks to information assets" (Da Veiga et al., 2007). The information security culture represents as

one of the necessary factor for effective information security management and without appropriate attention to security training and awareness for all ICT users, this cannot be achieved (Tarimo, 2006). Therefore, policy, awareness, training and education are some of the important factors that need to be established to ensure the security culture (Lim et al., 2010). As a result, it is clear that awareness and training programs play a major role for security culture. Therefore, there is a need to integrate awareness and education to ensure an effective security culture. Based on this discussion, the current study concluded security training has strong influence on creation of a security culture. Therefore, it has been included as a candidate factor for the research conceptual model.

2.6.1.7 Top Management Support

The most important factor affecting information security management activities in organizations is top management support (M. A. Alnatheer, 2012). The rank of top management support was number one in a list of 25 security issues that can affect information security (Knapp et al., 2007). However, the major issue that organizations face in daily operations is the lack of commitment from senior management (Barton, 2014). Fulford and Doherty (2003) stated that top management can be involved by defining and communicating a security policy, allocating specific responsibilities to appointed people, making resources available for the continual upkeep of information security and control, and constantly monitoring and reviewing information security effectiveness. In addition, top management support has been identified as the most important variable to contribute successful information security implementation. It has influence on information security effectiveness (M. A. Alnatheer, 2015). Many researchers have concluded that top management is an essential part of the security culture establishment (AlHogail & Mirza, 2014; M. A. Alnatheer, 2015; D'Arcy & Greene, 2009; Kraemer et al., 2009). M. A. Alnatheer (2015) indicated that top management support has significant influence on security culture. Without strong support from the top management of the organization the security culture would not be easily

established. Therefore top management support has been included as a candidate factor for the research conceptual framework.

2.6.1.8 Security Culture

The importance of creating a security culture within organization settings arises from the fact that the human dimension in information security is always considered to be the weakest link (Da Veiga & Eloff, 2010). Security culture reflects the values and beliefs of information security shared by all members at all levels of an organization (D'Arcy & Greene, 2009). Therefore, information security culture has been regarded as an important factor for supporting and guiding ISM practice (Chang & Lin, 2007). Many studies have concluded that the information security culture is important factor for implementing and establishing effective information security (S. M. Alfawaz, 2011; M. A. Alnatheer, 2014). To manage security effectively, there is need to create security culture. As a result, security culture would have strong influence on security effectiveness creation and has been included as a candidate factor for the research conceptual framework.

2.6.1.9 Information Security Structure

Information security structure refers to the extent to which the information systems are structured or dispersed throughout an organization (Knapp, 2005). Security mechanisms are the technologies that provide the security services (S. Alfawaz et al., 2008). Security will be established correctly if they begin with a complete planning of the information systems and organizations infrastructures (Pulkkinen et al., 2007). This has been indicated as one of information security necessities as stated by both.

Technical infrastructure that is capable of handling the required volume and type of transactions in a secure manner is a necessary for achieving the objectives of information security (S. M. Alfawaz, 2011). Dhillon and Backhouse (2000) argued that there is need

to understand the complex interplay between behavioral patterns and the technological structures to ensure proper security. Relevant information security infrastructures, in the context of this study, refer to the technologies that provide the security services. For example digital signatures, firewalls, antivirus, intrusion detection, and access control mechanisms. These types of technologies can help in providing confidentiality, integrity, authentication, and non-repudiation services for organizations' information security system (Katzan, 2012).

In terms of information security infrastructure, developing countries in general lack the necessary security technology structures (Sahi & Madan, 2012). Since the information security structures has a direct influence on information security management effectiveness (S. M. Alfawaz, 2011), therefore , information systems structure has been included as a candidate factor for the research conceptual framework.

2.7 Research Gaps

Recent studies (Aladwani, 2016; S. M. Alfawaz, 2011; AlKalbani et al., 2014; Huang & Farn, 2016; Jaafar et al., 2014; Naik et al., 2014; Oseni et al., 2015; Wangwe, 2012) have shown that securing systems such as e-government services is still a challenging and urgent issue that requires a variety of approaches. The surveyed literature has shown gaps that can be concluded as:

1. In general, overall results show that the lack of security is the most common problem faced by many e-government projects. E-government implementation faces various issues related to security and data protection. There are many governmental portals which have been subject to hacking. Therefore, there is an increased need to focus on this information protection and security. In this regard, the study enhances awareness and understanding of the importance to secure e-government services. It outlines the need of security requirements to be developed at the e-government implementation.

2. There is lack of discussion on information security from socio-technical perspective for e-government. As a result, the socio-technical attention to information security has been low compared to technical issues.
3. The literature review indicated the lack of comprehensive framework to guide the cultivation of an effective information security culture to improve the information security effectiveness. Most available framework were lacking in comprehensive view that integrated the human, the organization and the technology to provide comprehensive framework which aid the organization's information security practitioner in the implementation of an information security culture .
4. Lack of socio-technical and technical security requirements eGDMs stages. Therefore, there is a need to focus these issues into these eGDMs stages.
5. With respect to developing countries, there is a resulting lack of attention in the open literature on socio-technical factors such as the culture, ethical, organizational and level of awareness and how these factors relate to generic attitudes towards information security and its management.
6. Considering the general lack of empirical research and the importance of information security to modern organizations, this study seeks to contribute to the literature by developing and empirically testing an information security culture framework for securing e-government.

In general, the review of literature has concluded that still there is much to be developed in the information security field from socio-technical aspect. Therefore the security issues related to the human and processes components of information security management need to be focus. This showed the clear need to focusing on the socio-technical approach for securing e-government services. The next chapter will discuss the research methodology.

2.8 Chapter Summary

As discussed earlier, e-government implementation faces various issues related to security and data protection. Today, a vast body of research is available on this aspect and a lot of research has been done to provide secure transactions, to offer protection against hacker and various cyber attacks etc. However, information security is a critical issue facing organizations worldwide today. Therefore, there is an increased need to focus on this information protection and security related to delivery enabled services (ITGI, 2013). It has been noted that most of the researchers have dedicated their efforts to various areas of security researches. Their focus has been on technical side only and socio-technical attention to information security has been low compared to other information security issues (Shaaban, 2014; Wangwe, 2012). Lack of empirical research in the area of security from socio-technical point of view has also been concluded (S. M. Alfawaz, 2011; AlKalbani et al., 2014). Thus, different information security components such as human factors, organizational factors, and technical factors can be used to compile a new comprehensive information security framework.