ISSN 2278-5612

A Comparative Analysis of e-government security frameworks Social-Technical Security Aspect

Rabia Ihmouda[1] and Najwa Hayaati Mohd Alwi[2]
Universiti Sains Islam Malaysia (USIM) – Faculty of science and technology - Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
rbhamouda@yahoo.com
Universiti Sains Islam Malaysia (USIM) – Faculty of science and technology - Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
najwa@usim.edu.my

ABSTRACT

In recent years, most governments invested in the development of electronic government to improve government's efficiency and provide better services to businesses and citizens. As the successful implementation of the e-government depends on the viable security, all the concerns related to it need to be addressed. Security has become one of the crucial factors and primary challenges for achieving an advanced stage of e-government. In this regard, the paper investigates and analyzes six e-government security frameworks to assessing the security weaknesses of these frameworks from socio-technical security aspects. Meta-synthesis methodology used in this study, the meta-synthesis follows the steps used in meta-ethnography which adopted from Noblit and Hare. The finding is clearly showed that the socio-technical security missed to the rest of the security control principles and best practices elements. Therefore there is a clear need of a holistic socio-technical approach to be developed to match the pertinent security requirements into the e-government implementation.

Keywords

E-governments, E-Government security frameworks, Socio-technical security

INTRODUCTION AND BACKGROUND

E-government primarily refers to the use of information and communication technologies (ICT) in governmental organization processes. E-Government can be defined as – the electronic interaction (transaction and information exchange) between the government, the public (citizens and businesses) and employees [1].There are different categories of E-government. Carter & Belanger [2] mention four categories of e-government. These include: Government to Citizen (G2C), Government to Employee (G2E), Government to Government (G2G), and Government to Business (G2B) [2].

With increase use in e-government services on the Internet, the security related issues are also coming in the forefront, the information security is defined as 'the protection of information from a wide range of threats in order to minimize business risk and accordingly maximize return on investments and business opportunities, to ensure business continuity' [3].

The success of e-government requires facing all the challenges addressed in implementing e-government, especially the information security challenge. Security is one of the most important aspects of e-government systems. Typical security issues encompass trust, authentication and access control. The three basic security concepts, important to information on the Internet are confidentiality, integrity, and availability, all contribute to making the e-government environment a secure and save environment [4].

Standards play an essential role for drawing the roadmap of information security, ISO/IEC 17799:2005 is an essential standard for information security, the purpose of ISO/IEC 17799 is to assure the confidentiality, integrity and availability of information assets of the organization by setting guidelines for initiation, implementation, maintenance, and improvement of Information security management in an organization [5].

Security threats posed to e-government services could result from technical and/or socio-technical related issues, technical security aspects may include vulnerability caused by poor system design, development, implementation, configuration, integration (vertical and horizontal), and/or maintenance. Similarly, socio-technical security aspects may result from lack of ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and/or awareness program [6-9];[10].

In a research was carried out by Alfawaz et al [11] proposed a framework for understanding of the management issues involved in improving e-government security in developing countries. Kessler et al [12] introduced framework that includes five stages of e-government and their specific privacy requirements, technology and citizen requirements. Posthumus & Von Solms [13] introduced an effective framework for information security for government websites need to be encouraged, they had highlighted the importance of protecting business information for the organization, and the need for integrating information security into corporate governance through the development of an information security framework by investigating several fundamental considerations that should be taken into consideration in this regard.

The study is to find the security gaps of e-government security frameworks from socio-technical security aspects. It is investigates and analyzes six e-government security frameworks by using Meta-synthesis.

ISO STANDARDS

The International Organization for Standardization (ISO) Standards are designed to help organizations to effectively manage their information systems security [5]. ISO/IEC 27002:2005 is code of practice for information security management, which is another name of the ISO 17799 standard [15]. It provides best practices recommendations for those in charge of initiating, implementing and managing information systems security. ISO/IEC 27002 contains twelve major domains which deal with information security issues which include [16]:

- Security policy - management direction;
- Organization of information security - governance of information security;
- Asset management - inventory and classification of information assets;
- Human resources security - security aspects of employee joining and leaving organization;
- Physical and environmental security - protection of computer security;
- Communications and operations management - management of technical security;
- Access control - restriction of access control to systems, resources and network facilities;
- Information systems acquisition, development and maintenance - building security into applications;
- Information security incident management - anticipating and responding to security breaches;
- Business continuity management - protecting, maintaining and recovering business critical systems, processes and assets;
- Compliance - ensuring compliance with organizational standards, policies, rules and regulations, procedures and norms; and

- Risk assessment - analysis, planning, controlling and monitoring of implemented solutions and measures.

SOCIO-TECHNECAL APPROACH

The study was grounded on the theoretical foundation from the Socio-Technical approach (STA) and the Security By Consensus (SBC) model [6]. Socio-technical systems theory has been used for decades as a framework to design and understand organizations.

Socio-Technical Model (STM)

Kowalski [6] developed Socio-technical model (STM),the model is depicted in Figure 1. Suggests, an information system could be broken down into a socio and technical sub-system. The social subsystem can be sub divided into culture and structural sub systems. People using an information system have culture like ethics, traditions, laws and other social values. The technical part consists of methods and machines. Every system strives to be in balance so when any of the components or subsystems of the socio-technical system change then other components change too, to keep the balance.

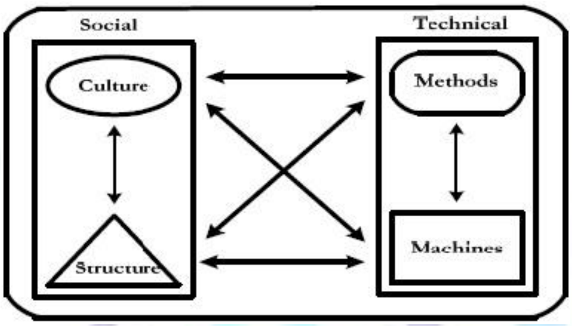

Fig 1: Socio-Technical Model (Kowalski, 1994, p.10)

SBC Model

To explicitly define the detailed parts of STM subsystem controls – the SBC model was applied detailed in Figure 2. In an IT system the social sub system can include ethical/cultural, legal/contractual, administrational managerial and operational procedural layers. The Technical sub system can include the following layers: mechanical/electronic; hardware; operating system; application; data, store, process, and collect information.

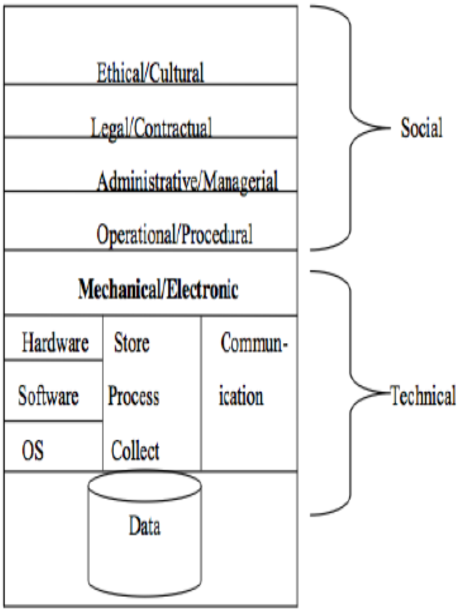

Fig 2: The basic SBC Model Kowalski [6]

A better model of security is the SBC model proposed by Kowalski [6] which gives a more useful description of security [14]. The SBC model can be used to analyze security at every level, from individual to national; this flexibility combined with the inclusion of the social elements meant that the SBC-model was the best fit for this study. The model divides with two basic components of a social subsystem and a technical subsystem, which are further divided into subclasses social (Ethical-cultural, Legal-contractual, Administrative-managerial-Policy, and Operational-procedural) and Technical (Mechanical-electronic and Information-Data). Tarimo who developed a mapping of security management domains in ISO 17799 with SBC model basis, this helps to easily comprehend security controls and issues at organizational level [15].

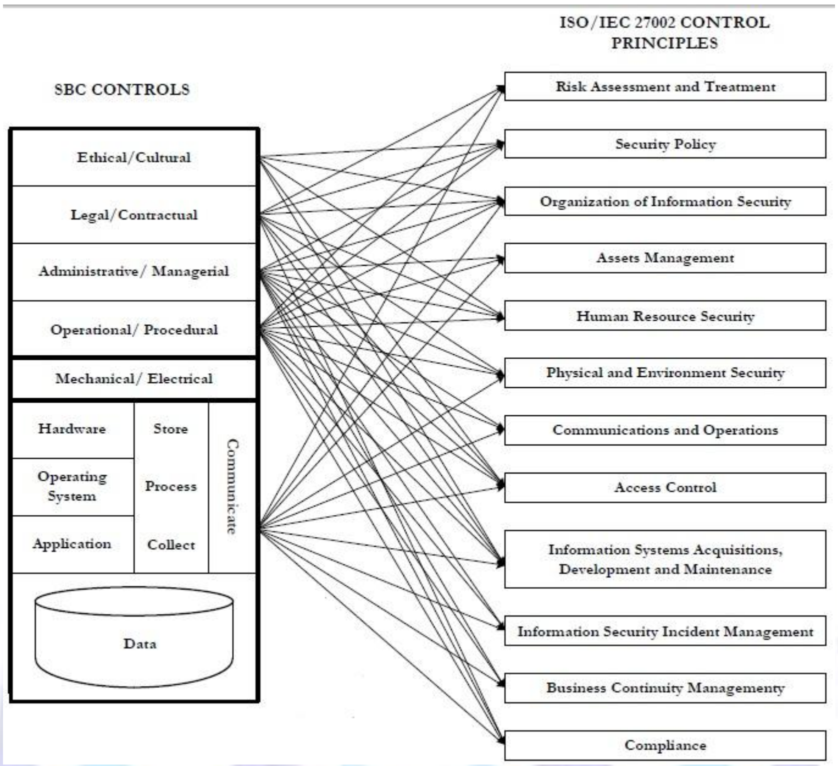
SBC CONTROLS
Ethical/Cultural
Legal/Contractual
Administrative/ Managerial
Operational/ Procedural
Mechanical/ Electrical
Hardware
Operating System
Application
Store
Process
Collect
Communicate
Data
ISO/IEC 27002 CONTROL PRINCIPLES
Risk Assessment and Treatment
Security Policy
Organization of Information Security
Assets Management
Human Resource Security
Physical and Environment Security
Communications and Operations
Access Control
Information Systems Acquisitions, Development and Maintenance
Information Security Incident Management
Business Continuity Managementy
Compliance

Fig 3: Mapping the Desired ICT Security Management State (ISO 17799) onto the SBC Model [15]

E-GOVERNMENT SECURITY FRAMEWORKS

E-Government framework is a guideline used by government organizations and businesses working with the government. Information security is a serious requirement which must be carefully considered .E-government security frameworks facilitate government organizations to effectively offer appropriate secure e-government services. Six e-government security frameworks will review in this section.

Kessler et al [12] proposed framework which aim to analyze the necessary requirements for privacy as a success factor in e-government systems. The framework identify major privacy-related issues in citizen-facing e-government systems and to develop appropriate recommendations for action, the framework's focus comes largely from a citizen perspective.

Belanger & Hiller [16] in their framework highlights the complex relationships that exist in e-government between the constituents and the government as various stages of e-government is implemented. The framework identify issues of privacy in e-government, analyze the effect of global motivators and constraints, and facilitate decision-making. This process is important to evaluate in depth complex issues, such as privacy in e-government.

Alfawaz et al [11] proposed a managerial conceptual framework for e-government security within the context of developing countries. The framework addresses related variables from security, cultural, managerial and organizational perspectives.

Al-Ahmad & Al-Kaabi [17] proposed an enhanced security framework that is designed especially for e-government systems. The framework is an essential tool that can be used by decision makers and designer of e-government systems. The framework considers all aspects of e-Government security, the people, processes and technologies.

Setiadi et al [18] proposed a comprehensive security framework that describes key components or elements to secure E-Government systems and processes. The proposed framework named Balanced e-Government Security Framework. This framework consists of multi-layer components such as (I) Asset layer, (2) Requirement layer, (3) Protection layer and key success factors for implementation information security. Protection layer is a layer described security control of E-Government. This layer consist three components such as administrative security, logical security and physical security.

Chetty & Coetzee [19] proposed a Service-oriented Architecture (SOA) information security framework, based on components, which consist of a variety of controls that can minimize the challenges of SOA information security. These components collectively provide direction for strategic, management/operational and technical levels to implement SOA information security.

METHODOLOGY

Meta-synthesis methodology attempts to integrate results from a number of different but inter-related qualitative studies. It is used to compare, interprets, translate, and synthesize different frameworks.

Meta-synthesis approach

Meta-synthesis method used in this study to provide interpretive translations, ground narratives or theories by integrating and comparing the findings of different qualitative studies [20] [21]. The study followed the seven-step meta-ethnography approach proposed by Noblit and Hare [22]:

Table1. Method steps

No	Method Steps	The Action
1	Identifying the research question	Identified our intellectual interest as studying e-government security frameworks in this step.
2	Identifying literature relevant to the research question.	This step is to systematically search through related databases and the internet to identify current literature related to e-government security framework. Six studies focusing on e-government security frameworks were identified.
3	Reviewing the selected studies	The papers were analyzed and studied repeatedly with special attention paid to the details of the interpretation of e-government security frameworks.
4	Determining how the studies are related.	This step is to find out the relationship between different accounts. Based on the analysis of the key concepts of each e- government security framework, the STM , SBC model [6], and the ISO/IEC 27002 twelve security control principles [ISO-27k] were identified as tools for guiding the development of the analysis criteria.
5	Translating the studies into one another.	This step is to conduct a comparison of key concepts between different studies so as to synthesize a comprehensive and integrated account. the investigated and analyzed each framework for the level of available security services was grounded on the theoretical foundation and building blocks from the STA and the SBC model [6]. Additionally, it utilizes the concepts ISO 27002 twelve security control principles [ISO-27K].
6	Synthesizing translations.	In this step, we further synthesized the translation and displayed of each framework with a Table 1.
7	Presenting the finding.	The results are explained in detail in this step

DEVELOPMENT PROCESS OF ANLYSIS CRITERIA

The development process of the evaluation criteria for the identified e-government security frameworks listed in Table 3 was grounded on the theoretical foundation and building blocks which discusses in section 4. To explicitly define the detailed part of the above ISO 27002 security control principles – it was mapped against the corresponding security assessment from the ISO 27002 best practices [ISO-27k]. Then each of the principle's assessment elements, defined in Table 2, was scaled to determine the level of available security services for each of the analyzed e-government security frameworks. Table 2 below depicts the detailed mapped ISO 27002 security control principles and their corresponding assessment elements.

Table2. Twelve ISO/IEC 27002 Security Control Principles and Best Practices Elements

No	ISO 27002 Security Control Principles Description [ISO-27k]	Best Practice Security Control Elements
1	Risk Assessment and Treatment	Security risk assessment
		Security risk analysis
		Security risk mitigation
2	Security Policy	Policies
		Guidelines and Procedures

		Principles and Standards
3	Organization of Information Security	Security Structures
		Security Reporting
		Security of third parties access
		Security outsourcing
4	Assets Management	Accountability for Assets
		Information classification
5	Human Resource Security	Security prior to employment
		Security during employment
		Security after change of employment
		Security awareness, training, and education
6	Physical and Environment Security	Physical access control
		Physical access monitoring
		Display media access control
		Equipment security control
		Environmental Control
7	Communications and Operations Management Security	Operational procedures and responsibilities
		Third party service delivery management
		Systems planning and acceptance
		Protection against malicious software
		Back-up
		Network security management
		Media handling security
		Information exchange security
		Electronic services security
		Monitoring logging and system use
8	Access Control	Business Requirement for access control
		User access management
		User responsibilities
		Network access control

		Operating systems access control
		Application and information access control
		Mobile computing and teleworking
9	Information Systems Acquisitions, Development and Maintenance	Security requirements of systems
		Security in application systems
		Cryptographic control
		Security of system files
		Security in development and support processes
		Technical vulnerabilities management
10	Information Security Incident Management	Reporting security events and weaknesses
		Management of security incidents & improvements
11	Business Continuity Management	Disaster Recovery Planning
		Resilience
12	Compliance	Legal requirements
		Security Policies
		Security Standards and Technical
		Systems Audit considerations

Analysis and Discussion

After developing the criteria for analyzing the identified e-government security frameworks for security services – we arranged the selected frameworks shown in Table 3 below. Further, we thoroughly investigated and analyzed each framework for the level of available security services.

Table3: Selected e-government security frameworks

No	Author	The framework	Proposed
1	Kessler et al	A Framework for Assessing Privacy Readiness of e-Government	Addresses relevant variables from policy, technology and citizen perspectives.
2	Belanger & Hiller	A framework for e-government: privacy implications	They illustrated the use of the framework to identify issues of privacy in e-government.
3	Alfawaz et al	a conceptual framework for e-government security management within the context of developing countries	Addresses related variables from security, cultural, managerial and organizational perspectives
4	Al-Ahmad & Al-Kaabi,	An Extended Security Framework for e-government	Addresses relevant variables from the people, processes and technologies perspectives
5	Setiadi et al.	Balanced E-Government	Include three layers: (1) Asset layer, (2) Requirement layer, (3) Protection layer and key

		Security Framework	success factors for implementation information security which consist three components such as administrative security, logical security and physical security.
6	Chetty & Coetzee	An Information Security Framework For Service-oriented Architecture	Consist of a variety of controls that can minimize the challenges of SOA information security strategic, management/operational and technical

Kessler et.al Framework

A Framework for Assessing Privacy Readiness of e-Government which proposed by Kessler et al [12], is consider three global constraints superimposed on these stages and relationship; laws and regulations, technical feasibility, and user feasibility. Additionally, when analyzing the framework based on the framework presented in Figure 3, and security control principles and best practices elements in Table2 the framework design had addressed socio-technical security services and related issues at a very low level. It is mentioned

- Policies element form Security Policy principle, Security prior to employment element from Human Resource Security principle, Business Requirement element from access control principle, Operational procedures and responsibilities element from Communications and Operations Management Security principle, Legal requirements element from Compliance principle. Further, the framework design did not consider the rest of the other security control principles and best practices elements. The table below summarizes the findings of the analysis.

Table 4. Available Social-Technical Security Services extracted in Kessler et al Framework

No	ISO 27002 Security Control Principles Description [ISO-27k]	Social-Technical Security			
		EC	LC	AM	OP
1	Security Policy	Policies	Policies	Policies	Policies
2	Human Resource Security	Security prior to employment	Security prior to employment	Security prior to employment	Security prior to employment
3	Communications & Operations Management Security			Operational procedures & responsibilities	Operational procedures & responsibilities
4	Access Control	Business Requirement for access control	Business Requirement for access control	Business Requirement for access control	Business Requirement for access control
5	Compliance		Legal requirements	Legal requirements	Legal requirements

***EC =Ethical/ Cultural, LC=Legal/ Contractual, AM=Administrative Managerial, OP=Operational Procedural**

Belanger & Hiller Framework

A framework for e-government: privacy implications which proposed by Belanger & Hiller [16], the framework is to identify issues of privacy in e-government. Additionally, when analyzing the framework based on the framework presented in Figure 3, and security control principles and best practices elements in Table 2 the framework design had addressed socio-technical security services and related issues at a very low level. It is only mentioned

- Policies element from Security Policy principle, Operational procedures and responsibilities element from Communications and Operations Management Security principle, Business Requirement element from access control principle, Security Policies element from compliance principle. Further, the framework design did not consider the rest of the other security control principles and best practices elements. The table below summarizes the findings of the analysis.

Table 5. Available Social-Technical Security Services extracted in Belanger & Hiller

No	ISO 27002 Security Control Principles Description [ISO-27k]	Social-Technical Security			
		EC	LC	AM	OP

1	Security Policy	Policies	Policies	Policies	Policies
2	Communications and Operations Management Security			Operational procedures and responsibilities	Operational procedures and responsibilities
3	Access Control	Business Requirement for access control	Business Requirement for access control	Business Requirement for access control	Business Requirement for access control
4	Compliance		Security Policies	Security Policies	Security Policies

Alfawaz et.al Framework

A conceptual framework for e-government security management within the context of developing countries which proposed by Alfawaz et al [11], The framework addresses related variables from security, cultural, managerial and organizational perspectives. Additionally, when analyzing the framework based on the framework presented in figure 3, and security control principles and best practices elements in Table2 the framework design had addressed socio-technical security services and related issues at a very low level. It is only mentioned

- Policies element from Security Policy principle, Security during employment element from Human Resource Security principle, Operational procedures and responsibilities element from Communications and Operations Management Security principle, User access management element from access control principle, Legal requirements element from compliance principle. Further, the framework design did not consider the rest of the other security control principles and best practices elements. The table below summarizes the findings of the analysis.

Table 6. Available Social-Technical Security Services extracted in Alfawaz et al

No	**ISO 27002 Security Control Principles Description [ISO-27k]**	**Social-Technical Security**			
		EC	**LC**	**AM**	**OP**
1	Security Policy	Policies	Policies	Policies	Policies
2	Human Resource Security	Security during employment	Security during employment	Security during employment	Security during employment
3	Communications and Operations Management Security			Operational procedures and responsibilities	Operational procedures and responsibilities
4	Access Control	User access management	User access management	User access management	User access management
5	Compliance		Legal requirements	Legal requirements	Legal requirements

Al-Ahmad & Al-Kaabi Framework

An Extended Security Framework for e-government which proposed by Al-Ahmad & Al-Kaabi [17], The framework addresses relevant variables from the people, processes and technologies perspectives. Additionally, when analyzing the framework based on the framework presented in Figure 3, and security control principles and best practices elements in Table2 the framework design had addressed socio-technical security services and related issues at a very low level. It is only mentioned

- Security during employment element from Human Resource Security principle, User access management element from access control principle. Further, the framework design did not consider the rest of the other security control principles and best practices elements. The table below summarizes the findings of the analysis.

Table 7. Available Social-Technical Security Services extracted in Al-Ahmad & Al-Kaabi [11]

	ISO 27002 Security Control	**Social-Technical Security**

No	Principles Description [ISO-27k]	EC	LC	AM	OP
1	Human Resource Security	Security during employment	Security during employment	Security during employment	Security during employment
2	Access Control	User access management	User access management	User access management	User access management

Setiadi et.al Framework

Balanced E-Government Security Framework which proposed by Setiadi et al [18], The framework include three layers: (1) Asset layer, (2) Requirement layer, (3) Protection layer and key success factors for implementation information security which consist three components such as administrative security, logical security and physical security. Additionally, when analyzing the framework based on the framework presented in Figure 3, and security control principles and best practices elements in Table 2 the framework design had addressed socio-technical security services and related issues at a very low level. It is only mentioned

- Security risk assessment element from Risk Assessment and Treatment principle, Guidelines and Procedures element from Security Policy principle, Accountability for Assets element from Assets Management principle, Security prior to employment from Human Resource Security principle, Physical access control element from Physical and Environment Security principle, Legal requirements element from compliance principle. Further, the framework design did not consider the rest of the other security control principles and best practices elements. The table below summarizes the findings of the analysis.

Table 8. Available Social-Technical Security Services extracted in Setiadi et al [18]

No	ISO 27002 Security Control Principles Description [ISO-27k]	Social-Technical Security			
		EC	LC	AM	OP
1	Risk Assessment and Treatment		Security risk assessment		Security risk assessment
2	Security Policy	Guidelines and Procedures	Guidelines and Procedures	Guidelines and Procedures	Guidelines and Procedures
3	Assets Management			Accountability for Assets	Accountability for Assets
4	Human Resource Security	Security prior to employment	Security prior to employment	Security prior to employment	Security prior to employment
5	Physical and Environment Security		Physical access control	Physical access control	Physical access control
6	Compliance		Legal requirements	Legal requirements	Legal requirements

Chetty & Coetzee Framework

An Information Security Framework For Service-oriented Architecture which proposed by Chetty & Coetzee [19], The framework consist of a variety of controls that can minimize the challenges of SOA information security strategic, management/operational and technical. Additionally, when analyzing the framework based on the framework presented in Figure 3, and security control principles and best practices elements in Table 2 the framework design had addressed socio-technical security services and related issues at a very low level. It is only mentioned

- Principles and Standards element from Security Policy principle, Accountability for Assets element from Assets Management principle. Security during employment element from Human Resource Security principle, Physical access control element from Physical and Environment Security principle, Reporting security events and weaknesses element from Information Security Incident Management principle, Security policy element from compliance principle. Further, the framework design did not consider the rest of the other security control principles and best practices elements. The table below summarizes the findings of the analysis.

Table 9. Available Social-Technical Security Services extracted in Chetty & Coetzee

No	ISO 27002 Security Control Principles Description [ISO-27k]	Social-Technical Security			
		EC	LC	AM	OP
1	Security Policy	Principles and Standards	Principles and Standards	Principles and Standards	Principles and Standards
2	Assets Management	■	■	Accountability for Assets	Accountability for Assets
3	Human Resource Security	Security during employment	Security during employment	Security during employment	Security during employment
4	Physical and Environment Security	■	Physical access control	Physical access control	Physical access control
5	Information Security Incident Management	■	■	Reporting security events and weaknesses	Reporting security events and weaknesses
6	Compliance	■	Security Policies	Security Policies	Security Policies

There were similar findings for the rest of the frameworks. The finding showed that it is imperative to include comprehensive security services that address socio-technical security requirements to secure the e-government services. It is clear to found that, the socio-technical security missed of the almost of the security control principles and best practices elements. In line this paper thoroughly investigates and analyzes six e-government security frameworks to assessing the socio-technical security weaknesses of e-government security frameworks, In this regard, the paper enhances awareness and understanding of the importance to having secure e-government services, it outlines the need of a holistic socio-technical approach to be developed to match the pertinent security requirements at the e-government implementation.

CONCLUSIONS AND FUTURE WORK

Securing e-government services appears to be a major challenge facing governments globally. This paper reviews six e-government security frameworks. Based on the literature review and conceptual analysis, the paper then discusses the socio-technical security gaps of each framework based on STM, SBC model [6], and the ISO/IEC 27002 security control principles [ISO-27k] and best practices elements in Table 2 were identified as tools for guiding the development of the analysis criteria. The findings of the analysis for e-government security frameworks has presented clearly showed that the socio-technical security missed of the almost of the security control principles and best practices elements. Therefore there is a clear need to a holistic cover for these requirements. The further research work will include developing socio-technical security framework services/ requirements for securing the e-government implementation.

REFERENCES

[1] Abramson, M.A. and G. Means, *E-government 2001, The Price water house Coopers endowment series on the business of government*. 2001, Lanham, Md.: Rowman & Littlefield.

[2] Carter, L. and F. Belanger, *The influence of perceived characteristics of innovating on e-government adoption.* Electronic Journal of E-government, 2004. **2**(1): p. 11-20.

[3] Mohd Alwi, N.H. and I.-S. Fan, *E-learning and information security management.* International Journal of Digital Society (IJDS), 2010. **1**(2): p. 148-156.

[4] Singh, S. and D.S. Karaulia. *E-Governance: Information Security Issues*. in *International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya*. 2011.

[5] ISO *ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems -- Requirements*. 2005.

[6] Kowalski, S., *IT Insecurity: A Multi-disciplinary Inquiry*. 1994: Univ.

[7] Gil-García, J.R. and T.A. Pardo, *E-government success factors: Mapping practical tools to theoretical foundations.* Government Information Quarterly, 2005. **22**(2): p. 187-216.

[8] A. Martins and J. Elofe. *Information security culture.* . in *Proceedings of IFIP TC11, 17th international conference on information security (SEC2002)*. 2002. Cairo, Egypt.: Springer US.

[9] Michael, Whitman, and H.J. Mattord, *Principles of Information Security,*. 3rd Edition ed. 2007.

[10] Wimmer, M. and B. Von Bredow. *A holistic approach for providing security solutions in e-government*. in *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*. 2002. IEEE.

[11] Alfawaz, S., L.J. May, and K. Mohannak, *E-government security in developing countries: A managerial conceptual framework.* 2008.

[12] Kessler, K., et al. *A Framework for Assessing Privacy Readiness of e-Government.* . 2011.

[13] Posthumus, S. and R. Von Solms, *A framework for the governance of information security.* Computers & Security, 2004. **23**(8): p. 638-646.

[14] Nohlberg, M., *Social engineering: understanding, measuring and protecting against attacks*. 2007, ph. d. Licenciature, dept. Hum. And inf., univ. Of skövde, sweden.

[15] Tarimo, C.N., *ICT security readiness checklist for developing countries: A social-technical approach*. 2006, Stockholm.

[16] Belanger, F. and J.S. Hiller, *A framework for e-government: privacy implications.* Business process management journal, 2006. **12**(1): p. 48-60.

[17] Al-Ahmad, W. and R. Al-Kaabi. *An extended security framework for e-government*. in *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*. 2008. IEEE.

[18] Setiadi, F., Y.G. Sucahyo, and Z.A. Hasibuan. *Balanced E-Government security framework: An integrated approach to protect information and application*. in *Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2013 International Conference on*. 2013. IEEE.

[19] Chetty, J. and M. Coetzee. *Towards an information security framework for service-oriented architecture*. in *Information Security for South Africa (ISSA), 2010*. 2010. IEEE.

[20] Beck, C.T., *A meta-synthesis of qualitative research.* MCN: The American Journal of Maternal/Child Nursing, 2002. **27**(4): p. 214-221.

[21] Sandelowski, M., S. Docherty, and C. Emden, *Focus on qualitative methods Qualitative metasynthesis: issues and techniques.* Research in nursing and health, 1997. **20**: p. 365-372.

[22] Noblit, G.W. and R.D. Hare, *Meta-ethnography: Synthesizing qualitative studies*. Vol. 11. 1988: Sage.