International Journal of Engineering & Technology, *8 (1.10) (2019) 186-191*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Identifying the role of Information Systems to implement Information Security System

[1]Dr Siew Poh Phung, [2]Assoc. Prof. Dr. Valliappan Raju, [3]Tuan Haji Zanial

[1]Manager---Academics, Limkokwing University, [2]Sr. Lecturer, Limkokwing University [2]Sr.Lecturer, Limkokwing University

Abstract

Given that data forms a crucial resource in the contemporary world, especially in situations such as those involving handling crime, guidelines or benchmarks have evolved to support the security of the data. This paper presents different forms of data security principles and culminates into an examination of crucial data security measures that are worth embracing. Specific data security guidelines that the paper presents include COBIT, ITIL, PCIDSS, BS 7799, AND ISO27001. The study's central objective is to highlight a state of standardization and position that the respective standards exhibit, as well as different countries' appropriations and the ease of use of these guidelines.

Key Words. *Information Security System, Implementation*

1. Introduction

In many organizations, information or data forms a backbone of operations (including business firms), a trend coming in the wake of increasing incorporation of information technology (IT) applications into company operations. This trend has been informed by the need for quicker access to and the retrieval of data, especially during key administrative decision-making processes. Therefore, it becomes important to tailor data framework assets to assure security.

Notably, data security stretched beyond passwords and usernames [5]. For organizations, data security assurance remains a key consideration towards achieving own missions and visions [6]. The growing need has been informed by frequent cases of data breaches involving social architects, phishers, programmers, and worms. From the insights in figure 1, intrusions continue to yield enormous losses among organizations; especially due to the loss of customer data, as well as business ideas or internal company data [7]. In response to such dangers, there is a growing need for organizations to embrace executive frameworks in data security, ISMS inclusive. The latter framework constitutes features responsible for enhancing the security of personal computers based on the programming assets of the equipment or device. Particularly, the framework strives to manage the utilization of the PC assets to avoid data insecurity.

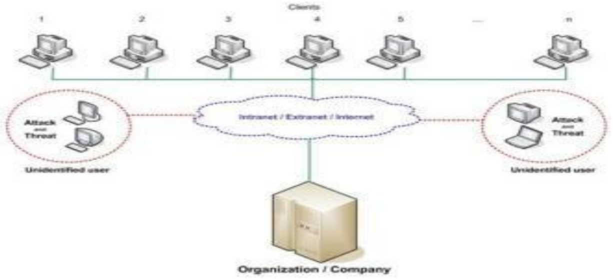


Fig1: Data Network

Given that organizational processes are supported through data security, benchmarks or standards are needed to control administrative functions targeting the data security practice. Hence, some private and public firms have evolved to establish regulations that yield the perceived benchmarks; especially regarding data access and use. Some of the IT governance models that have been documented include COBIT, ITIL, SOA, COSO, PCIDSS, BS7799, ISO27001, PMMM, P-CMM, CMMI, OPM3, and PRINCE2. Imperative to note is that not all the models mentioned above have gained global application. The current paper focuses on five major models. These models include COBIT, ITIL, PCIDSS, BS7799, and ISO27001. The motivation is to investigate the qualities of these frameworks, as well as principles governing their functionality.

2. Isms standards

This section reviews the five major data security models mentioned above. As highlighted earlier, the models are investigated relative to the parameters of the models' profiles, as well as the approaches that they embrace to execute the ISMS role with which they are associated. The figures presented in this section also aid in comprehending the positions, practices, and capacities of the selected data security models.

2.1. ISO27001

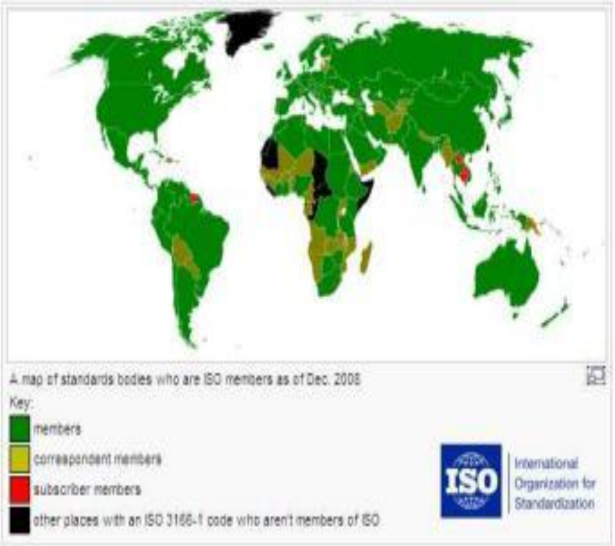

A map of standards bodies who are ISO members as of Dec. 2008
Key:
🟩 members
🟨 correspondent members
🟥 subscriber members
⬛ other places with an ISO 3166-1 code who aren't members of ISO
ISO
International Organization for Standardization

Fig 2: ISO Classification

ISO evolved in 1947 when business and contemporary measures were declared on February 23rd. the declaration was made in the context of Geneva, Switzerland [8]. Recent statistics indicate that this framework has its presence in 163 countries (see Figure 2). Its initiation was informed by the need to establish, execute, work, observed, assess, and keep abreast with ISMS reporting [25].

Notably, ISO strived to foster security control among data sources. As such, it has gained application in various organizations among local and international industries, including private and public firms. Its associated cyclic model involves a "Plan---Do---Check---Act" (PDCA) show [1], which is charged with enhancing, executing, screening, and establishing organizational viability [2].

2.2. BS 7799

This model was established in 1995 and distributed by the British Standard Institution (BSI) Group [13], [16]. It initial segment involves accepted ISMS procedures while a modified version, which emerged in 1998, incorporated a data technology code through which data security training would be implemented. In 1999, BSI also established and distributed another version that entailed data security management systems especially in relation to the board structure and data control.

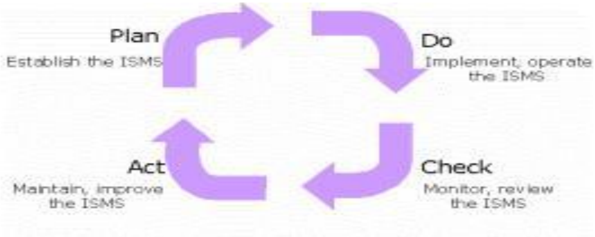


Fig 3: PDAC Model

2.3. PCIDSS

The emergence of the Payment Card Industry Data Security Standard (PCIDSS) came in the wake of growing interest in data security models within the Payment Card Industry Security Standards Council. Its initiation was also informed by a quest to enable industry players establish card installments and also assume total control of customer data; including Visa information. Imperatively, this framework is applicable to organizations from different industries, especially those that trade, process, or possess cardholder information from various cards containing the card brands' logos [20]. The model is illustrated in Figure 4.

Regarding consistency, approval via the use of this model tends to be achieved remotely. However, factors that determine the framework's efficiency include the nature or size of the organization, the volume of card exchanges or transactions. Notably, the framework calls for annual evaluations and reviews to discern consistency in system performance. It is also worth indicating that this model gains application in situations involving organizations that handle vast amounts of data or data exchanges. These volumes are also assessed for consistency by using the Qualified Security Assessor (QSA) approach [21]. For institutions that handle smaller volumes of information, a Self-Assessment Questionnaire (SAQ) remains at their disposal as a framework through which consistency with the provisions of the selected type of data security framework can be assessed.

2.4. ITIL

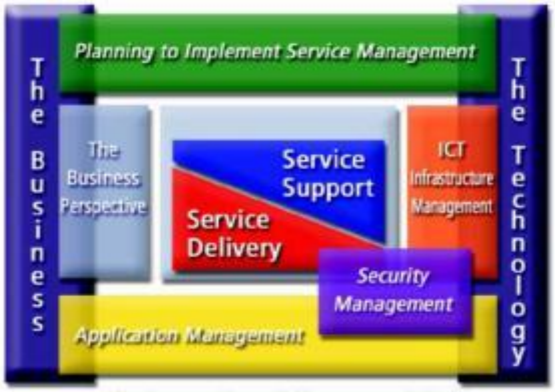


Fig 4: Implementing Service Management

The idea of the Information Technology Infrastructure Library (ITIL) arose during the 1980s. At the time, the British government established that the benefits with which IT had come remained inadequate [19]. Indeed, ITIL reflects a practice and information arrangement aimed at serving IT activities and the Information Technology Services Management (ITSM), Information Technology (IT) improvement and IT activities, with a central objective being to enhance the security of these platforms.

Indeed, the model evolved as a collection of different books that highlighted IT service management practices or approaches. With the information combined, a procedure through which tasks could be controlled regularly was developed, with the effort spearheaded by W. Edwards Deming [4]. As illustrated in Figure 4, this model exhibits eight essential components. The components include small-scale implementation, planning towards service management implementation, software asset management, application management, security management, and ICT infrastructure management. Others include service delivery and service support.

2.5. COBIT

1.The Control Objectives for Information and related Technology (COBIT) is an affirmation made by ISACA and the IT Governance Institute (ITGI) in 1996 [9]. They trust that it is an arrangement of practices (system) for IT the executives. COBIT is an IT administration structure and supporting toolset that enables administrators to cross over any barrier between control necessities, specialized issues, business dangers, and security issues. COBIT has five IT Governance zones of fixation [12], [23]: Strategic arrangement centers around guaranteeing the linkage of business and IT designs; characterizing, keeping up and approving the IT offer; and adjusting IT tasks to big business activities.

2.Value conveyance is tied in with executing the incentive all through the conveyance cycle, guaranteeing that IT conveys the guaranteed advantages against the procedure, focusing on streamlining costs and demonstrating its inborn estimation.

3.costs and demonstrating its inborn estimation.

4.Resource the executives is about the ideal venture and the best possible administration of basic IT assets: applications, data, framework and individuals.

4.Risk managementis a reasonable comprehension of the venture's hunger for hazard, comprehension of consistence necessities, and straightforwardness into the association.

5.Performance estimation tracks and screens methodology execution, venture consummation, asset use, process execution and administration conveyance, for instance, adjusted scorecards that make an interpretation of procedure enthusiastically to accomplish objectives quantifiable past regular bookkeeping.

3. Highlights

Alfantookh2009 [2], characterized 11 fundamental control called by 11EC, that ought to be actualized by an association, as necessities and consistence of the data security criteria by the standard collection of ISMS [2], [6] because of these highlights as premise of parameters and benchmarks for satisfaction of data security which is most completely cover all viewpoints must be claimed, these 11EC are [8], [24]:

Data Security Policy: how an establishment communicates its plan with underlined to data security, implies by which an organization's overseeing body communicates its goal to anchor data, provides guidance to the executives and staff and educates alternate partners of the power of endeavors.

Correspondences and Operations Management: characterized arrangement on security in the association, in lessening security hazard and guaranteeing right registering, including operational methods, controls, and all around characterized obligations.

Access Control: is a framework which empowers a specialist to control access to zones and assets in a given physical office or PC based data framework.

Data System Acquisition, Development and Maintenance: an incorporated procedure that characterizes limits and specialized data frameworks, starting with the obtaining, and improvement and the latter is the support of data frameworks. AAssociation of Information Security: is a structure possessed by an association in executing data security, comprises of; the board promise to data security, data security co---appointment, approval process for data handling offices. Two noteworthy bearings: interior association, and outer gatherings.

Resource Management: depends on the possibility that it is critical to recognize, track, characterize, and appoint proprietorship for the most essential advantages for guarantee they are satisfactorily secured.

Data Security Incident Management: is a program that plans for occurrences. From an administration point of view, it includes recognizable proof of assets required for episode taking care of. Great occurrence the board will likewise help with the avoidance of future episodes.

Business Continuity Management: to guarantee coherence of activities under irregular conditions. Plans advance the status of foundations for fast recuperation despite unfriendly occasionsor conditions, limit the effect of such conditions, and give intends to encourage working amid and after crises.

HR Security: to guarantee that all representatives (counting contractual workers and client of touchy information) are fit the bill for and comprehend their jobs and obligations of their activity obligations and that get to is expelled once business is ended.

Environmental and physical security: Indeed, these attributes target the supporting foundation, structures, and frameworks relative to the physical condition that ought to curb against potential harm or unauthorized access to the frameworks and associated data.

4. Comparisonsof thebig five

In this case, profiles with which different standards are associated are highlighted. The aim is to reflect the position of each guideline in relation to global utilization.

Currently, standards and guidelines gain global recognition or acknowledgment based on their capacity to support organizational management (see Figure 6). Examples of such standards include COBIT in one nation, ITIL in one nation, PCIDSS in one nation, BS in one nation, and ISO in 25 nations.
[Figure7] The most widely adopted guideline, ISO, is experienced in 163 countries compared to COBIT in 160, ITIL in 50, PCIDSS in 125, and BS in 110 countries. Hence, ISO remains more effective and has gained application among senior executives, clients or customers, and providers.

One of the dynamic standards, BS, has been deemed superior to ISO, as well as COBIT, ITIL, and PCIDSS. However, standards such as COBIT, PCIDSS, and ISO exhibit some features that are also superior to BS [13]. Notably, most of the partners or stakeholders have continually favored standards that prove to be progressively adaptable. Those that have proved to exhibit this features include COBIT, PCIDSS, and ISO. It is also worth highlighting that in data security, BS7799 and ISO 27001 exhibit similar qualities because the form arose from the latter and only reflects an enhanced version. The remainders of the standards focus on aspects of project management and IT administration (see Figure 8).

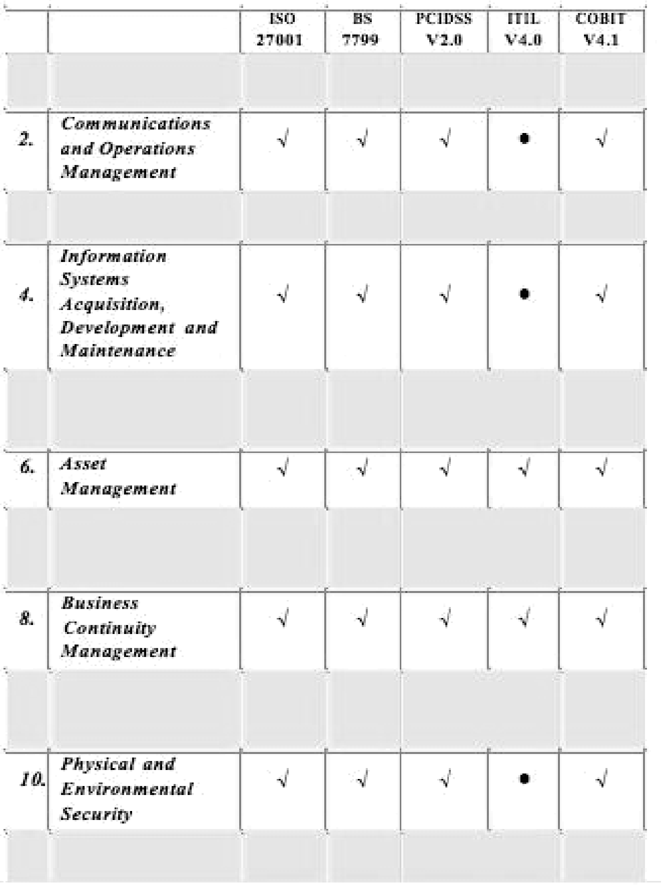
5. Conclusion

In summary, different standards govern different job positions regarding ISMS execution. Examples include BS 7799 and ISO 27001, which target data security . on the other hand, PCIDSS strives to govern business exchanges and savvy cards, with COBIT and ITIL targeting data security and how it correlates with IT governance and project execution (see Figure 8). Notably, ISO 27001 has been found to drive at least four guidelines, especially in relation to ISMS. The eventuality is that it (ISO 27001) is more effective and continues to be preferred by stakeholders such as controllers, clients or customers, providers, the staff, and senior administrators.

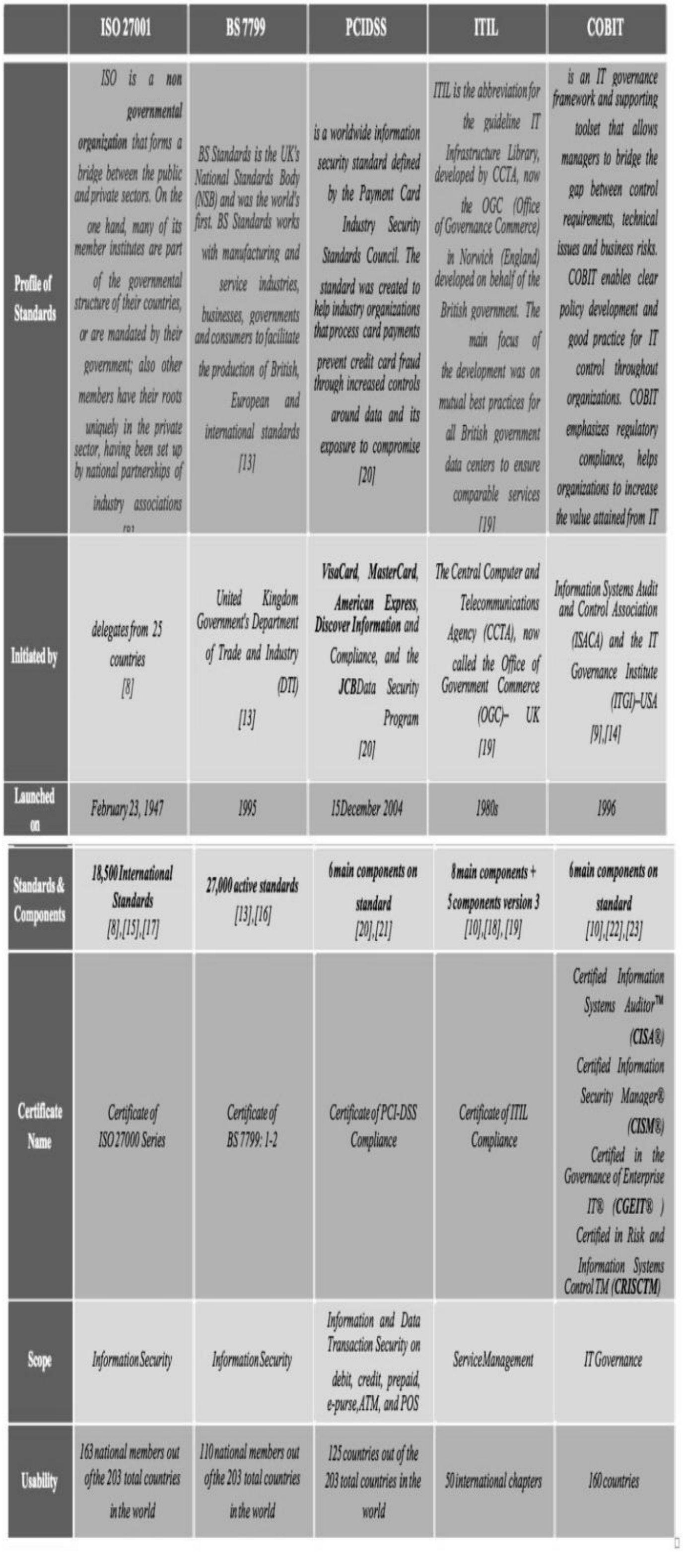
Recommendation

Based on the insights gained form this study, there is a need to refine ISO (27001). Specifically, the refinement needs to ensure that partners from different organizations execute their roles and also collaborate accordingly. It is recommended further that the refinement transforms and deciphers abnormal state dialects in relation to ISMS appraisals, with individual speeches on focus.

Table 1 below we showed up head to head comparisons on the big five ISMS standards deal with 11EC of information security.



		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
2.	***Communications and Operations Management***	√	√	√	●	√
4.	***Information Systems Acquisition, Development and Maintenance***	√	√	√	●	√
6.	***Asset Management***	√	√	√	√	√
8.	***Business Continuity Management***	√	√	√	√	√
10.	***Physical and Environmental Security***	√	√	√	●	√



	ISO 27001	BS 7799	PCIDSS	ITIL	COBIT
Profile of Standards	*ISO is a **non governmental organization** that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government; also other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations [8]*	*BS Standards is the UK's National Standards Body (NSB) and was the world's first. BS Standards works with manufacturing and service industries, businesses, governments and consumers to facilitate the production of British, European and international standards [13]*	*is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help industry organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise [20]*	*ITIL is the abbreviation for the guideline IT Infrastructure Library, developed by CCTA, now the OGC (Office of Governance Commerce) in Norwich (England) developed on behalf of the British government. The main focus of the development was on mutual best practices for all British government data centers to ensure comparable services [19]*	*is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT*
Initiated by	*delegates from 25 countries [8]*	*United Kingdom Government's Department of Trade and Industry (DTI) [13]*	***VisaCard, MasterCard, American Express, Discover Information** and Compliance, and the **JCB**Data Security Program [20]*	*The Central Computer and Telecommunications Agency (CCTA), now called the Office of Government Commerce (OGC)– UK [19]*	*Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)–USA [9],[14]*
Launched on	*February 23, 1947*	*1995*	*15December 2004*	*1980s*	*1996*
Standards & Components	***18,500 International Standards** [8],[15],[17]*	***27,000 active standards** [13],[16]*	***6main components on standard** [20],[21]*	***8main components + 5components version 3** [10],[18], [19]*	***6main components on standard** [10],[22],[23]*
Certificate Name	*Certificate of ISO 27000 Series*	*Certificate of BS 7799: 1-2*	*Certificate of PCI-DSS Compliance*	*Certificate of ITIL Compliance*	*Certified Information Systems Auditor™ (**CISA®**) Certified Information Security Manager® (**CISM®**) Certified in the Governance of Enterprise IT® (**CGEIT®**) Certified in Risk and Information Systems Control TM (**CRISCTM**)*
Scope	*InformationSecurity*	*InformationSecurity*	*Information and Data Transaction Security on debit, credit, prepaid, e-purse,ATM, and POS*	*ServiceManagement*	*IT Governance*
Usability	*163 national members out ofthe 203 total countries inthe world*	*110national members out ofthe 203 total countries inthe world*	*125 countries out of the 203 total countries in the world*	*50 international chapters*	*160 countries*

Tabel 2. *Profile of Big Five of ISMS Standards*

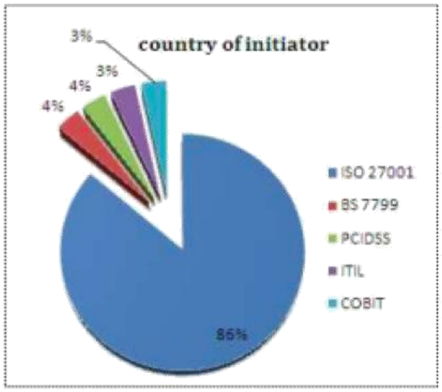


Figure 6. *Country as initiator of standard*

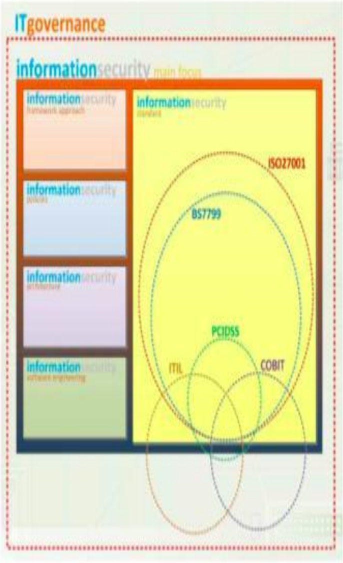


Figure 8. *Position of each standard*

References

[1] Alan Calder and Setve Watkins. IT Governance – A Manager’s Guide to Data Security and ISO 27001 and ISO 27002

[2] Abdulkader Alfantookh. An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls.

[3] Computer Sciences, King Saud University. 2009

[4] Basie von Solms. 2005. Information Security Governance: COBIT or ISO 17799 or both? Computer&Security Journal. Elsevier.Science Direct Basie von Solms. 2005. Information Security Governance – Compliance Management vs Operational Management. Computer & Security Journal. Elsevier, Science Direct Basie von Solms & Rossouw von Solms. 2004. The 10 deadly sins of Information Security Management. Computer & Security 23(2004) 371--- 376. Elsevier Science Ltd.

[5] Heru Susanto & Fahad bin Muhaya. Multimedia Information Security Architecture. @ IEEE. 2010.

[6] Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan.

[7] I---SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution’s Six Domains. Journal of Computer, Asian Transaction. July 2011.

[8] ISO History and Definition. www.iso.org

[9] IT Governance Institute. COBIT 4.1 Excerpts. 2007. Rolling Meadows,

[10] IT Governance Institute. Mapping of ITIL v3 with COBIT 4.1. 2008.

[11] Rolling Meadows, IL 60008 USA

[12] The Government of the Hong Kong. An Overview of Information Security Standards. 2008. Hongkong.

[13] Overview on COBIT. http://www.benchmarklearning.com/COMMUNITIES/ITIL/cobit.aspx.