Information Security Management System Standards: A Comparative Study of the Big Five

Information Security Management System Standards: A Comparative Study of the Big Five

Heru Susanto[12], **Mohammad Nabil Almunawar**[1] and **Yong Chee Tuan**[1]

[1]FBEPS, University of Brunei
Information System Group
susanto.net@gmail.com & 10h0103@ubd.edu.bn

[2]The Indonesian Institute of Sciences
Information Security & IT Governance Research Group
heru.susanto@lipi.go.id

Abstract. -- It cannot be denied that nowadays information is a very important asset for any modern organization. Therefore protecting its security is very important and becoming a top priority for many organizations. Unfortunately there is no single formula that can guarantee 100% of information security. Therefore there is a need for a set of benchmarks or standards to ensure the best security practices are adopted and an adequate level of security is attained. In this paper, authors introduce various information security standards briefly and then provide a comparative study for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. The study will provide a picture of the position and specialization of each standard, adoption by countries and their usability levels.

Keywords– ISO27001, BS7799, PCIDSS, ITIL, COBIT, ISMS, Information Security, PDCA

I. Introduction

Information is the lifeblood of organizations, a vital business asset in today's Information Technology (IT) -enabled world. Access to high-quality, complete, accurate and up-to-date information is vital in supporting managerial decision-making process that leads to sound decisions. Thus, securing information system resources is extremely important to ensure that the resources are well protected. Information security is not just a simple matter of having usernames and passwords [5]. Regulations and various privacy / data protection policy impose a raft of obligations to organizations [6]. Meanwhile viruses, worms, hackers, phishers and social engineers threaten organizations on all sides. Hackers or sometimes we call edit by unidentified user is likely to cause huge losses for an organization [figure 1], such as by theft of customer data, spy on business strategy, for the benefit of competitors [7]. It is imperative for organizations to use an information security management system (ISMS) to effectively manage their information assets. ISMS is basically consist of sets of policies put place by an organization to define, construct, develop and maintain security of their computer based on hardware and software resources. These policies dictate the way in which computer resources can be used.

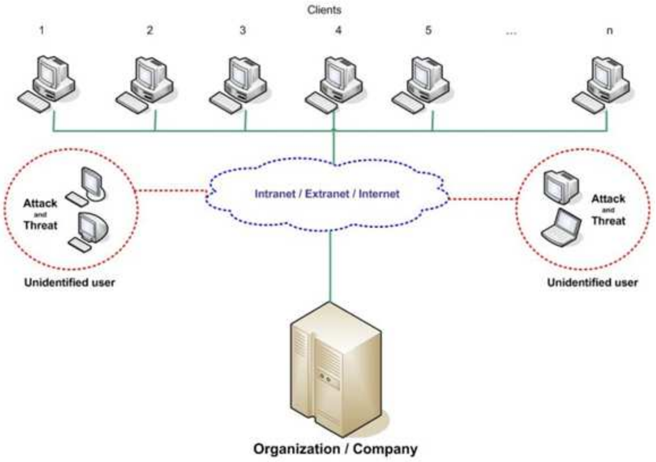

Figure 1. *Activities of unidentified user as potential attack and threat to organization*

Since information security has a very important role in supporting the activities of the organization, we need a standard or benchmark which regulates governance over information security. Several private and government organizations developed standards bodies whose function is to setup benchmarks, standards and in some cases, legal regulations on information security to ensure that an adequate level of security is preserved, to ensure resources used in the right way, and to ensure the best security practices adopted in an organization. There are several standards for IT Governance which leads to information security such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT.

However, some of these standards are not well adopted by the organizations, with a variety of reasons. In this paper we will discuss the big five of ISMS standards, widely used standards for information security. The big five are ISO27001, BS 7799, PCIDSS, ITIL and COBIT. This comparative study conducted to determine their respective strengths, focus, main components and their adoption based on ISMS.

II. ISMS Standards

This section we give an overview of the big five ISMS standards; ISO27001, BS7799, PCIDSS, ITIL and COBIT. The overview includes profile and methodology used in each standard in implementing ISMS for organizations. These overviews will help readers easily understand functions, behaviors and position of each on the big figure and whole ISMS's strategies.

II.1. ISO27001

ISO, founded on February 23, 1947, promulgates worldwide proprietary industrial and commercial standards, has headquarters in Geneva, Switzerland [8]. It has 163 national members out of the 203 total countries in the world [figure 2]. The international standard of ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within an organization [25].

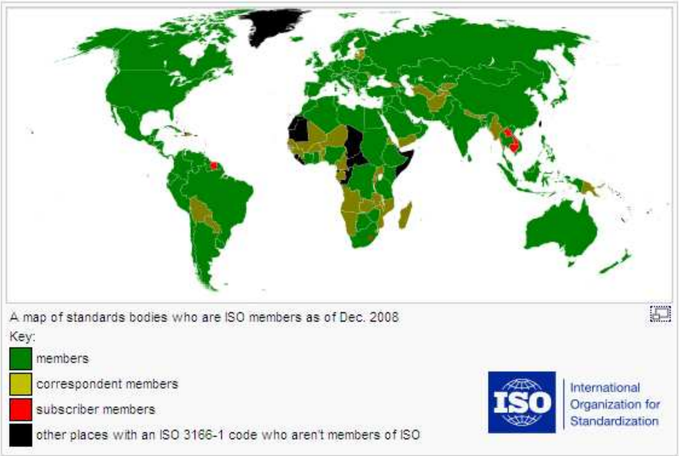
A map of standards bodies who are ISO members as of Dec. 2008
Key:
🟩 members
🟨 correspondent members
🟥 subscriber members
⬛ other places with an ISO 3166-1 code who aren't members of ISO
ISO
International Organization for Standardization

Figure 2. *Map of members of ISO* (***by IchwanPalongengi***)

It designed to ensure the selection of adequate and proportionate security controls to protect information assets. This standard is usually applicable to all types of organizations, either private or public organizations. The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model [1], aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS [2].

II.2. BS 7799

BS 7799 was a standard originally published by British Standard Institution (BSI) Group in 1995. It was written by the United Kingdom Government's Department of Trade and Industry (DTI), and consisted of several parts [13], [16]. The first part, containing the best practices for ISMS, was revised in 1998, which was eventually adopted by ISO as ISO17799, "*Information Technology - Code of practice for information security management*." The second part of BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "*Information Security Management Systems - Specification with guidance for use*", BS 7799-2 focused on how to implement ISMS, referring to the information security management structure and controls identified in BS 7799-2, which later became ISO 27001. The 2002 version of BS 7799-2 introduced the Plan-Do-Check-Act (PDCA) (Deming quality assurance model) [figure 3], aligning it with quality standards such as ISO 9000. BS 7799 Part 2 was adopted by ISO as ISO 27001 in November 2005 [16].

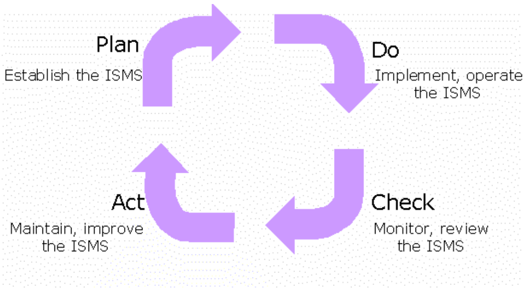

Figure 3. *PDCA Model on BS 7799*

II.3. PCIDSS

The Payment Card Industry Data Security Standard (PCIDSS) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help industry organizations processes card payments and to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands [20], [figure 4].

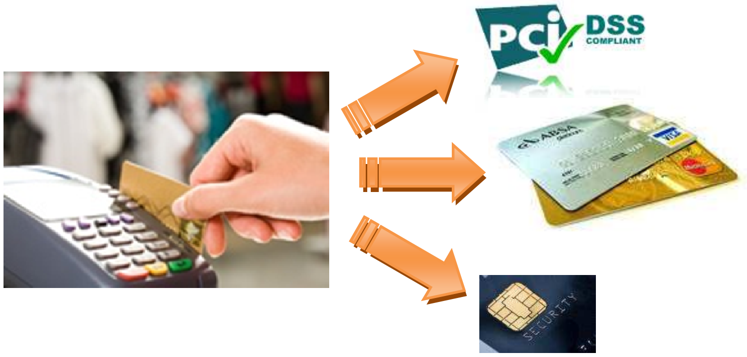

Figure 4. *Transaction security models of PCIDSS*

Validation of compliance can be performed either internally or externally, depending on the volume of card transactions, but regardless of the size of the organization, compliance must be assessed annually. Organizations handling large volumes of transactions must have their compliance assessed by an independent assessor called by Qualified Security Assessor (QSA) [21], while companies handling smaller volumes have the option of demonstrating compliance via a Self-Assessment Questionnaire (SAQ).

II.4. ITIL

The Information Technology Infrastructure Library (ITIL) concept emerged in the 1980s, when the British government determined that the level of IT service quality provided to them was not sufficient [19]. ITIL is a set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations, which has parts focus on security.

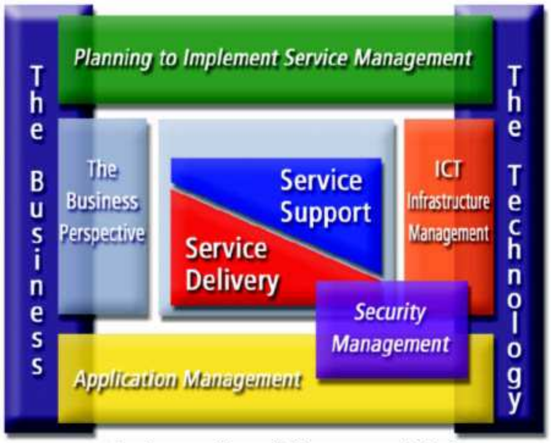

Figure 5. *The ITIL components*

The ITIL originated as a collection of books, each covering a specific practice within IT Service Management, was built around a process-model based view of controlling and managing operations often credited to W. Edwards Deming and his plan-do-check-act (PDCA) cycle [4], as IT Services Management Standards and Best Practices [18] contains of 8 main components[figure 5], they are: Service Support, Service Delivery, ICT Infrastructure Management, Security Management, Application Management, Software Asset Management, Planning to Implement Service Management, Small-Scale Implementation.

II.5. COBIT

The Control Objectives for Information and related Technology (COBIT) is a certification created by ISACA and the IT Governance Institute (ITGI) in 1996 [9]. They believe that it is a set of practices (framework) for IT management. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues. COBIT has five IT Governance areas of concentration [12], [23]:

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

- **Resource management** is about the optimal investment and the proper management of critical IT resources: applications, information, infrastructure and people.

- **Risk management**is a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, and transparency into the organization.

- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

III. Features

Alfantookh2009 [2], defined 11 essential control, *called by 11EC*, that should be implemented by an organization, as requirements and compliance of the information security criteria by the standard body of ISMS [2], [6] due to these features as basis of parameters and benchmarks for fulfillment of information security which is most comprehensively cover all aspects must be owned, these 11EC are [8], [24]:

1. ***Information Security Policy:*** how an institution expresses its intent with emphasized to information security, means by which an institution's governing body expresses its intent to secure information, gives direction to management and staff and informs the other stakeholders of the primacy of efforts.

2. ***Communications and Operations Management:*** defined policy on security in the organization, in reducing security

risk and ensuring correct computing, including operational procedures, controls, and well-defined responsibilities.

3. ***Access Control*****:** is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system.

4. ***Information System Acquisition, Development and Maintenance*****:** an integrated process that defines boundaries and technical information systems, beginning with the acquisition, and development and the last is the maintenance of information systems.

5. ***Organization of Information Security:*** is a structure owned by an organization in implementing information security, consists of; management commitment to information security, information security co-ordination, authorization process for information processing facilities. Two major directions: internal organization, and external parties.

6. ***Asset Management*****:** is based on the idea that it is important to identify, track, classify, and assign ownership for the most important assets to ensure they are adequately protected.

7. ***Information Security Incident Management:*** is a program that prepares for incidents. From a management perspective, it involves identification of resources needed for incident handling. Good incident management will also help with the prevention of future incidents.

8. ***Business Continuity Management:*** to ensure continuity of operations under abnormal conditions. Plans promote the readiness of institutions for rapid recovery in the face of adverse events or conditions, minimize the impact of such circumstances, and provide means to facilitate functioning during and after emergencies.

9. ***Human Resources Security:*** to ensure that all employees (including contractors and user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated.

10. ***Physical and Environmental Security:*** to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment, buildings and rooms that house information and information technology systems must be afforded appropriate protection to avoid damage or unauthorized access to information and systems.

11. ***Compliance:*** these issues necessarily are divided into two areas; the first area involves compliance with the myriad laws, regulations or even contractual requirements which are part of the fabric ofevery institution. The second area is compliance with information security policies, standards and processes.

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
1.	***Information Security Policy***	√	√	√	√	√
2.	***Communications and Operations Management***	√	√	√	●	√
3.	***Access Control***	√	√	√	√	√
4.	***Information Systems Acquisition, Development and Maintenance***	√	√	√	●	√
5.	***Organization of Information Security***	√	√	√	√	√
6.	***Asset Management***	√	√	√	√	√
7.	***Information Security Incident Management***	√	●	√	√	√
8.	***Business Continuity Management***	√	√	√	√	√
9.	***Human Resources Security***	√	√	√	●	√
10.	***Physical and Environmental Security***	√	√	√	●	√
11.	***Compliance***	√	√	√	√	√

Tabel 1. *Features of Big Five of ISMS Standard*

IV. COMPARISONSOF THEBIG FIVE

Profile of each standard is presented here to provide a general overview and summaryof the relevant standard on their respective positions which is currently most widely used worldwide [table 2].

	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 [9]
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	15 December 2004	1980s	1996
Standards & Components	**18,500 International Standards** [8],[15],[17]	**27,000 active standards** [13],[16]	**6 main components on standard** [20],[21]	**8 main components + 5 components version 3** [10],[18], [19]	**6 main 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	Information Security	Information Security	Information and Data Transaction Security on debit, credit, prepaid, e-purse, ATM, and POS	Service Management	IT Governance
Usability	163 national members out of the 203 total countries in the world	110 national members out of the 203 total countries in the 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*

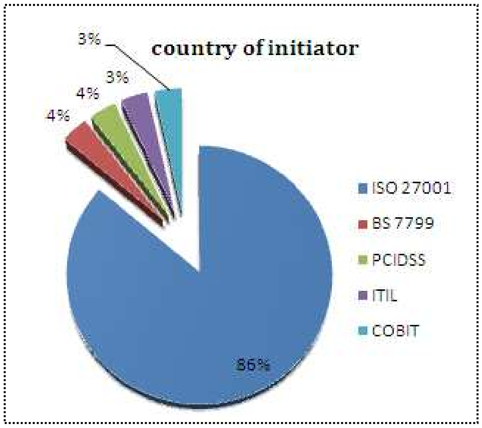

Figure 6. *Country as initiator of standard*

Nowadays, it is very important for a standard, accepted and recognized as global benchmarking tools, marked by number of county which initiated for establishment of an organization deal with [figure 6]. ISO (25 countries) BS (1 country) PCIDSS (1 country), ITIL (1 country), and COBIT (1 country).

[Figure7] ISO's most widely used in globally by163 countries, compared with BS (110), PCIDSS (125), ITIL (50) and COBIT (160). Indication descript us that ISO is more easily implemented, stakeholders (clients, suppliers, customers and management) is easier to recognize, also it has appropriate platform in an organization deal with, than four others security standards.

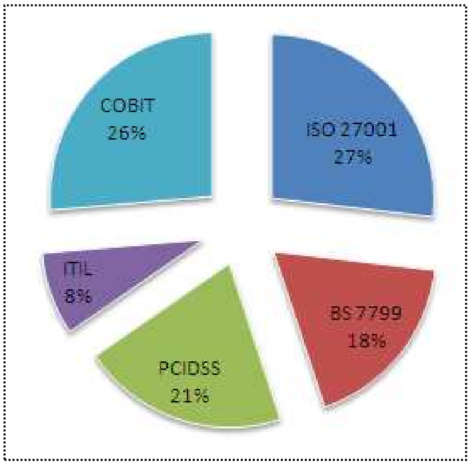

Figure 7. *Usability level of standards*

Substantively numbers of active standard on BS is 50% more than the standard that is owned by ISO, and also more than PCIDSS, ITIL and COBIT, but other reason that leads organization not implemented BS, tend to preferred ISO, PCIDSS, COBIT is due in some part BS using benchmarks Europe or commonly known as BSEN (British Standard Europe Norm) [13], inauspiciously it would confuse stakeholders, which one is better, BS or BSEN, local or regional, such as pouring the same water in two glasses of different shapes. Stakeholders prefer a more flexible standard, more focus and have not two different terms for the same issues; thus, ISO, PCIDSS, COBIT become more consideration as best choice.

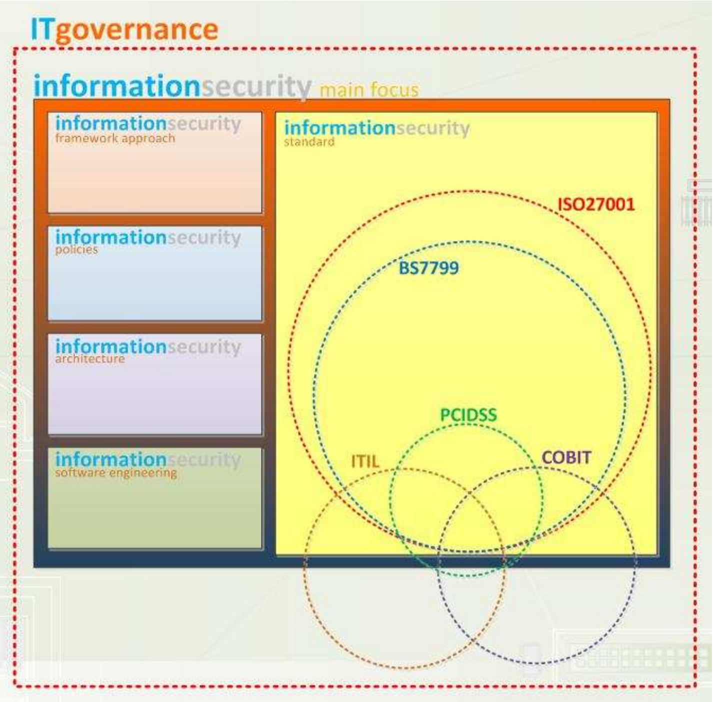

Figure 8. *Position of each standard*

The main focus on information security, ISO27001 and BS7799 have similar characteristics, since ISO27001 adopted from BS7799, with improvements and additions emphasized on the strength of ISMS from various aspects, while the three others also focus on IT governance and Project Management [figure 8].

V. Conclusion Remarks

Each standard playing its own role and position in implementing ISMS, several standards such as ISO 27001 and BS 7799 focusing on information security management system as main domain and their focus on, while PCIDSS focus on information security relating to business transactions and smart card, then ITIL and COBIT focuses on information security and its relation with the Project management and IT Governance [figure 8]. Refers to the usability of standards in global, indicated that ISO (27001) leading than four other standards especially on ISMS, therefore it described us the standard is more easily implemented and well recognized by stakeholders (top management, staff, suppliers, customers/clients, regulators). We can analogous ISO (27001) is like a global language in standards and benchmarking on ISMS, such as English as an international language, with level of usability and trust reach more than 80% of the world [figure 2].

VI. Recommendation and Future Research

As the international language of standards and recognized globally, authors recommend further research in refinement of ISO (27001). Purposed of refinement is to make more easily understood, implemented, and easily measured in an organization by stakeholders. Refinement expected translating and interpreting high level language of terms, technical nature and details on the subject of ISMS assessments to understandable human being parlance.

VII. Acknowledgment

This paper is one part of the big research which topic of framework for refinement information security management system as tools of integrated solutions. This research is supported by FBEPS University of Brunei Darussalam (UBD), The Indonesian Institute of Sciences and Prince Muqrin Chair (PMC) for IT Security, King Saud University (KSU).

VIII. 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. Computer Sciences, King Saud University. 2009

[3] Basie von Solms. 2005. Information Security Governance: COBIT or ISO 17799 or both? Computer&Security Journal. Elsevier.Science Direct

[4] Basie von Solms. 2005. Information Security Governance – Compliance Management vs Operational Management. Computer & Security Journal. Elsevier, Science Direct

[5] Basie von Solms & Rossouw von Solms. 2004. The 10 deadly sins of Information Security Management. Computer & Security 23(2004) 371-376. Elsevier Science Ltd.

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

[7] Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan. *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, IL 60008 USA

[10] IT Governance Institute. *Mapping of ITIL v3 with COBIT 4.1*. 2008. Rolling Meadows, IL 60008 USA

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

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

[13] Overview on British Standard. *http://www.bsigroup.com/en/Standards-and-Publications/About-BSI-British-Standards/*

[14] *http://www.isaca.org/KnowledgeCenter/COBIT/Pages/Overview.aspx*

[15] *http://www.iso.org/iso/about/discover-iso_isos-name.htm*

[16] *http://www.isms-guide.blogspot.com/2007/11/key-components-of-standard-bs-7799-iso.html*

[17] *http://www.iso.org/iso/about.htm*

[18] *http://www.itil.org/en/vomkennen/itil/ueberblick/index.php*

[19] *http://www.itil-officialsite.com/faq.aspx?category=General+FAQs&btnSubmit=Open*

[20] *https://www.pcisecuritystandards.org/security_standards/index.php*

[21] *http://www.retrievernpc.com/cms/pci-compliance/certificate-of-pci-dss-compliance/*

[22] *http://technet.microsoft.com/en-us/library/ff758651.aspx*

[23] *http://searchsecurity.techtarget.com/feature/Introduction-to-COBIT-for-SOX-compliance*

[24] *https://wiki.internet2.edu/confluence/display/itsg2/ Human+Resources+Security+(ISO+8)*

[25] *http:// wikipedia.org/wiki/ISO*

Heru Susanto is a researcher at The Indonesian Institute of Sciences, Information Security & IT Governance Research Group, also was working at Prince Muqrin Chair for Information Security Technologies, Information Security Research Group, King Saud University. He received BSc in Computer Science from Bogor Agriculture University, in 1999 and MSc in Computer Science from King Saud University, nowadays he as PhD Candidate in Information System from the University of Brunei Darussalam. Heru has published many papers in refereed journals as well as international conferences.

Mohammad Nabil Almunawar is a senior lecturer at Faculty of Business, Economics and Policy Studies, University of Brunei Darussalam. He received master Degree (MSc Computer Science) from the Department of Computer Science, University of Western Ontario, Canada in 1991 and PhD from the University of New South Wales (School of Computer Science and Engineering, UNSW) in 1997. Dr Nabil has published many papers in refereed journals as well as international conferences. He has many years teaching experiences in the area computer and information systems. He was a respected consultant in developing information systems for United Nations (WHO) projects, Central Bank of Indonesia and some private companies. His overall research interest is application of IT in Management and Electronic Commerce. He is also interested in object-oriented technology, databases and multimedia retrieval.

Yong Chee Tuan is a senior lecturer at Faculty of Business, Economics and Policy Studies, University of Brunei Darussalam, has more than 20 years of experience in IT, HRD, e-gov, environmental management and project management. He received PhD in Computer Science from University of Leeds, UK, in 1994. He was involved in the drafting of the two APEC SME Business Forums Recommendations held in Brunei and Shanghai. He sat in the E-gov Strategic, Policy and Coordinating Group from 2003-2007. He is the vice-chair of the Asia Oceanic Software Park Alliance. He has been appointed as the regular judge of the APICTA since 2001. He is the country representative in the UNDP Digital Review Publications.