The Egyptian Int. J. of Eng. Sci. and Technology
Vol. 15, No. 2 (May 2012)

EIJEST

DEVELOPING AN EVALUATION FRAMEWORK FOR INFORMATION SYSTEM SECURITY VIA ISO 17799 MODEL*

Abdel-Nasser H. Zaied**
College of Computers and Information, Zagazig University, Egypt

ABSTRACT

Information system security (ISS) plays an important role in protecting the assets of an organization. The functioning of modern organizations is increasingly reliant on computers and global networks. In such organizations, ISS aimed at ensuring the confidentiality; integrity; and availability of information. So, organizations need practical security benchmarking tools in order to plan effective security strategies. Evaluating information systems security is a process which involves identifying; gathering; and analyzing security functionality and assurance level against certain standards. This can result in a measure of trust that indicates how well the system meets a particular security target. This paper attempts to provide an interpretation of ISO/IEC 17799, 2005 (ISO/IEC 27002) applications by adapting an evaluation framework for organization information system security level. An empirical study is performed to aid in validating the used framework. The results show that the framework is helpful for decision makers to decide the priorities and courses of actions should be taken to improve the organization security maturity level.

KEYWORDS: Organization information system security; Information system security evaluation framework; ISO 17799 Model; ISO/IEC 27002 Model.

ÉLABORATION D'UN CADRE D'ÉVALUATION DE LA SÉCURITÉ SYSTÈME D'INFORMATION VIA ISO 17799 MODÈLE

RESUME

Système d'information de sécurité (ISS) joue un rôle important dans la protection des actifs d'une organisation. Le fonctionnement des organisations modernes est de plus en plus dépendants des ordinateurs et des réseaux mondiaux. Dans ces organisations, l'ISS visant à assurer la confidentialité, l'intégrité, et la disponibilité des informations. Ainsi, les organisations ont besoin des outils d'étalonnage pratiques de sécurité afin de planifier des stratégies de sécurité efficaces. Évaluation des systèmes d'information de sécurité est un processus qui consiste à identifier, recueillir les données et l'analyse de la fonctionnalité de sécurité et de niveau d'assurance contre certaines normes. Il peut en résulter une mesure de confiance qui indique dans quelle mesure le système répond à un objectif de sécurité particulier. Ce document tente de donner une interprétation de la norme ISO / CEI 17799, 2005 (ISO / IEC 27002) les applications en adaptant un cadre d'évaluation pour les informations sur l'organisation de la sécurité au niveau du système. Une étude empirique est réalisée afin d'aider à la validation du cadre utilisé. Les résultats montrent que le cadre est utile pour les décideurs de décider des priorités et des cours des actions devraient être prises pour améliorer le niveau de maturité organisation de la sécurité.

MOTS-CLES: la sécurité du système d'information Organisation; information sur l'évaluation du système de sécurité-cadre; ISO 17799 Modèle; ISO / CEI 27002 Modèle.

* Received: 29/1/2011, accepted: 11/4/2012 (Original Paper)

** Contact author (nasserhr@zu.edu.eg, nasserhr@gmail.com)

1. INTRODUCTION

The increased utilization of information systems and the Internet has brought security issues to the fore. Information system has become a critical issue, so, organizations need high standards of excellence for protection of information assets and information technology resources that support all levels in the organizations. Without the implementation of appropriate controls and security measures, these assets are subject to potential damage or compromise to confidentiality or privacy and the activities of the organizations are subject to interruption. This paper explores a number of techniques that can be used to measure security within an organization and proposes an evaluation framework to evaluate organization information system security level based on ISO/IEC 17799:2005 standard.

2. STANDARDS FOR INFORMATION SECURITY

Standards play an essential role for drawing the roadmap of information security. In 2002 OECD developed guidelines for the security of information systems consisted of: accountability; awareness; ethics; multidisciplinary; proportionality; integration; timeliness; reassessment; and democracy (OECD, 2002). NIST (1995) suggested seven principles for developing a IS security awareness. These principles are: identify program scope; goals and objectives; identify training staff; identify target audience; motivate management and employees; administer the program; maintain the program; and evaluate the program. In 1998, NIST presented a conceptual framework for providing different roles relative to the use of information systems. The framework segmented an employee's organizational role into six functional specialties: manage; acquire; design and develop; implement and operate; review and evaluate; and use (NIST, 1998 & NIST, 2003). In December 2000, International Organization for Standardization (ISO) established guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (ISO/IEC 17799, 2005), an enhanced version of ISO/IEC 17799 appeared in late 2005 (ISO/IEC 27001, 2005 & ISO/IEC 27002, 2005). ISO 17799, provides a detailed list of controls that can be used for establishing an information security program. This standard contains guidelines and best practices recommendations for 11 security domains: security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; and compliance.

3. INFORMATION SYSTEM SECURITY EVALUATION

After published ISO 17799 in year 2000, many researchers suggested guidelines and frameworks to support design; implementation and evaluation of information system security (Katsikas, 2000; Tudor, 2001; Peltier, 2002; René, 2005; Solms, 2005; Villarroel et al. 2005; Savola & Roning, 2006 and Karabacak & Sogukpinar, 2006). Later on, Wiander (2007) analyzed the implementation experiences of four organizations that have implemented the ISO/IEC 17799 (2005) standard. The results of the study suggested that the ISO/IEC 17799 standard is commonly viewed as a necessary element in information security management. Also, it was concluded that there is a need for a more agile framework for implementing the ISO/IEC 17799 standard in practice. Yan (2008) developed a

security evaluation approach for information systems in telecommunication enterprises based on: access paths, which evaluated system security through analyzing user behavior patterns and utilizing product evaluation results. Recently, Dzazali et al.(2009) evaluated the information security maturity level of the Malaysian Public Service (MPS) organizations. A survey questionnaire was utilized to gauge the security level and to further understand the occurrence of incidents; the sources of attack; and the types of technical safeguard. Lai and Dai (2009) provided an implementation guidance of network isolation (referring to ISO-17799 standard) in two aspects (technique viewpoints and management viewpoints) to revise the implementation security plan for information security level in government departments in Taiwan. They concluded that ISO-17799 mentions the methods of "segregation in networks" in the control and the implementation guidance for the network security measures. These methods employ security facilities and protection techniques to ensure the network security of departments. Zaied (2009) suggested a priority indexing model (PIM) to evaluate organization's information security system and to calculate a development priority index that can be used as an indicator for system development needs. He concluded that the proposed model may assist decision makers to consider different criteria and indicators before committing to a particular choice of security system development or to evaluate any existing security system. Yang et al. (2009) established a security evaluation system for 12 network enterprises in Beijing and evaluated security level using the method of combining the qualitative with the quantitative, and overcome the subjectivity in the evaluation through the application of self-adapting regression Support Vector Machine (SVM). More recently, Wallace et al. (2011) examined the extent to which the information technology (IT) controls suggested by the ISO 17799 security framework have been integrated into organizations' internal control environments. They summarized the results only on a list of the ten most commonly implemented controls. The survey results also indicated that control implementation differences exist based on a company's status as public or private, the size of the company, and the industry in which the company operates. Training of IT personnel is also associated with significant differences in implemented controls.

4. EVALUATION FRAMEWORK

Many related standards and guidelines have been drawn up for the effective assessment of security levels. Security experts uniformly agree that there is no such thing as a 100 % secure information system. To better understand how organizations are applying information security, we developed a survey to gauge the participants' perceptions of the prevalence of specific information security elements, as outlined by the most comprehensive standard, ISO/IEC 17799, in their organizations.

4.1 Methodology

A number of best practice frameworks exist to help organizations assess their information security risks. In this study, we chose to focus on the ISO 17799 framework of IT controls in order to examine current security practices for the following reasons:

- It is an internationally recognized, structured methodology;
- It directly focuses on information security, while other frameworks have a broader focus and provides the details on how to develop and implement these components; and
- It defines process to evaluate, implement, maintain, and manage information security, and includes procedures for measuring the security level of an organization and deriving the maturity of it by analyzing the measured data.

Table (1) shows the 11 main sections, 39 control objectives, and 133 detail control items used for checking of security level. These items cover information security measures that should be implemented by organizations, including organizational, physical and technical controls (ISO/IEC 27007, 2005) & ISO/IEC 27000, 2009).

Table (1): ISO/IEC 17799 Category Descriptions (As mentioned in Standard)

Main Sections (MS)	Control Objectives (CO)	Control Items (CI)
1- Security policy	1. Information security policy	**2**
2- Organizing information security	2. Internal Organization	**8**
	3. External Parties	**3**
3- Asset management	4. Responsibility for assets	**3**
	5. Information classification	**2**
4- Human resources security	6. Prior to employment	**3**
	7. During employment	**3**
	8. Termination or change of employment	**3**
5- Physical and environmental security	9. Secure Areas	**6**
	10. Equipment Security	**7**
6- Communications and operations management	11. Operational Procedures and responsibilities	**4**
	12. Third party service delivery management	**3**
	13. System planning and acceptance	**2**
	14. Protection against malicious and mobile code	**2**
	15. Backup	**1**
	16. Network Security Management	**2**
	17. Media handling	**4**
	18. Exchange of Information	**5**
	19. Electronic Commerce Services	**3**
	20. Monitoring	**6**
7- Access control	21. For Access Control	**1**
	22. User Access Management	**4**
	23. User Responsibilities	**3**
	24. Network Access Control	**7**
	25. Operating system access control	**6**
	26. Application and Information Access Control	**2**
	27. Mobile Computing and teleworking	**2**
8- Information systems acquisition, development and maintenance	28. Security requirements of information systems	**1**
	29. Correct processing in applications	**4**
	30. Cryptographic controls	**2**
	31. Security of system files	**3**
	32. Security in development and support processes	**5**
	33. Technical Vulnerability Management	**1**
9- Information security incident management	34. Reporting information security events and weaknesses	**2**
	35. Management of information security incidents and improvements	**3**
10- Business continuity management	36. Information security aspects of business continuity management	**5**
11- Compliance	37. Compliance with legal requirements	**6**
	38. Compliance with security policies and standards, and technical compliance	**2**
	39. Information Systems audit considerations	**2**

4.2 Proposed Evaluation Framework

Survey evaluation is based on the quantitative measures. To evaluate a survey, it is necessary to convert survey questions and answer choices into the numerical values. This task can be done by converting the opinions of employees of a company on its security into a hard number for an understanding of where security is weakened using the proposed evaluation Framework. The proposed evaluation Framework was developed based on ISO/IEC 17799:2005 as follows:

$$CIML_{lji} = \sum_{p=1}^{5}(ML_p * No.of\ participant)/5 * Total\ No.of\ participant \quad \ldots\ldots. \quad (1)$$

Control Objectives Maturity Level is equal to the summation of maturity levels for all Control Items according to their degree of importance.

$$COML_{ji} = \sum_{l=1}^{m}(CIML_{lji} * IC_l)/m \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

Standard Sections Maturity Level is equal to the summation of maturity levels for all Control Objectives according to their degree of importance.

$$SSML_i = \sum_{j=1}^{n}(COML_{ji} * IS_j)/n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

Organization Security Maturity Level is equal to the summation of maturity levels for all Standard Sections according to their degree of importance.

$$OSML = \sum_{i=1}^{k}(SSML_i * IO_i)/k \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

The general form can be derived by substituting equations 1, 2 and 3 in equation 4 as follows:

$$OSML = \sum_{i=1}^{k}((\sum_{j=1}^{n}((\sum_{l=1}^{m}(CIML_{lji} * IC_l)/m) * IS_j)/n) * IO_i)/k \quad (5)$$

Where:

OSML ≡ Organization Security Maturity Level
SSML ≡ Standard Sections Maturity Level
COML ≡ Control Objective Maturity Level
CIML ≡ Control Items Maturity Level
ML ≡ Maturity Level
I ≡ Degree of importance (if any and specified by organization)
k ≡ No. of Standard Sections (11 Sections)
n ≡ No. of Control Objectives in each Standard Sections (39 Objectives)
m ≡ No. of Control Items in each Control Objective (133 Items)
IC ≡ Control Item
IS ≡ Control Objective
IO ≡ Main Section

5. CASE STUDY

The main goal of this paper is to identify the current perceptions of information system security maturity level within organizations. This goal required surveying security practitioners and other employees within a variety of businesses. Organizations under study were of diverse sizes as indicated by the number of employees, but almost half were currently working at medium size firms. Respondents had varying degrees of experience and most have worked for more than five years. Respondents were asked to rate their perception towards the information

system security maturity level within their organizations. The organizations that form the sample was selected from Egyptian private companies that have an Intranet and willing to offer e-services. After personal contact, three organizations agreed to participate in the study conditioning to hide their names. The organizations were working in telecommunication, business and public services.

5.1 Research Tool

To examine the validity of the proposed evaluation framework, a simple questionnaire was designed; the number of controls in ISO 17799 limits the number of questions in the questionnaire. Thus, the number of questions was 133; a sample from the questions is shown in Table (2). The participants required to evaluate the maturity level (from 1 very low to 5 very high) of organization's information security system.

5.2 Sample Size

Three companies working in IT field where selected; their agreement to participate in the survey is only selection criterion. Emails were sent to IT managers to distribute the questionnaire to thirty participants in their companies and follow-up telephone calls and Emails were used to encourage them to complete and return it via Email. The average participants' experiences were between 5 and 15 years and had been employed by their current organization at least from five years.

Table (2): Sample of audit Check List according to BS ISO/ IEC 17799:2005
(Maturity Level 1 = very low - Level 2 = Low - Level 3 = Moderate - Level 4 = High - Level 5 = Very high)

Standard No.	Section	Explanations	Maturity Level				
			1	2	3	4	5
Security Policy							
5.1	**Information security policy**						
5.1.1	**Information security policy document**	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees. Whether the policy states management commitment and sets out the organizational approach to managing information security.					
5.1.2	**Review of Informational Security Policy**	Whether the Information Security Policy is reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness. Whether the Information Security policy has an owner, who has approved management responsibility for development, review and evaluation of the security policy. Whether any defined Information Security Policy review procedures exist and do they include requirements for the management review. Whether the results of the management review are taken into account. Whether management approval is obtained for the revised policy.					
Organization of information security							
6.1	**Internal Organization**						
6.1.1	**Management commitment to information security**	Whether management demonstrates active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities.					
6.1.2	**Information security coordination**	Whether information security activities are coordinated by representatives from diverse parts of the organization, with pertinent roles and responsibilities.					

6. RESULTS AND DISCUSSION

Ninety questionnaires (thirty for each company) were received. The success of the adopted framework adoption depends on the answers of participants, accurately answered questions lead to accurate results. The percentage of participants' opinions and the weighted average of maturity levels are shown in Table (3). The results show that the strengths in the organization information system security are: resources backup: (3.45) item No.10.5; human resources security prior to employment: (3.45) item No. 8.1; information systems audit considerations: (3.44) item No. 15.3; cryptographic controls: (3.42) item No. 12.3; and user access management: (3.4) item No. 11.2. Also, it show that the weaknesses may affect the system security are: technical vulnerability management: (2.87) item No. 12.6; third party service delivery management: (2.9) item No. 10.2; protection against malicious and mobile code: (2.98) item No. 10.4 and mobile computing and teleworking: (2.98) item No. 11.7.

After adopting the used framework, the results show some differences among the three organizations under study. The organization working in telecommunication services (organization-C) is the most commonly implemented security system and has high ISS maturity level, but organizations in Business (organization-B) and Services (organization-A) rated lower ISS maturity level as shown in table (4) and figure (1). The highest standards for all the three organizations are compliance and organization of information security (3.29) whereas the lowest one is security policy (3.10).

The results also show that the opportunities to improve organization security maturity level laying on improving security policy and Information systems acquisition, development and maintenance in organization A; security policy and Communications and Operations Management B and security policy and Information systems acquisition, development and maintenance in organization C.

7. CONCLUSIONS

Security is just like air. It is originally worthless, but its existence will not be painfully detected until it is lost. ISO/IEC 17799 compliance provides important advantages on many levels. ISO/IEC 17799 certification serves as a public statement of an organization's ability to manage information security. In this paper, an evaluation framework of information system security maturity level was adopted to reach the vision "Information resources can be fully used in an obstacle free and secure environment". The used framework demonstrates to partners and clients that the organization has implemented adequate information security and business continuity controls. It also demonstrates the organization's commitment to ensuring that its information security management system and security policies continue to evolve and adapt to changing risk exposures. Although other security studies have captured information about organizational size, none of them appear to have used that information to examine a relationship between organizational size and control implementation decisions. The analysis revealed that organizational size did not have a significant influence over whether a respondent could provide a "very high/very low" response to the survey questions as opposed to a "moderate" response. The used framework takes into account the variations of ISS levels in the organizations. Depending on the type of the organization, and the type of the processes within the organization, some clauses and questions in the clauses can be omitted. It does not have special requirements about the ISS; it can be used as a tool for continuous control of the security of information systems. Also, it is a helpful tool for decision makers to decide the priorities of courses of actions should be taken to improve organization security maturity level.

Table (3): Participants' opinions

Standard / Section	Organization Security Maturity Level *(OSML)* (weighted average)			
	Org. (A)	**Org. (B)**	**Org. (C)**	**Total**
5.0: Security Policy				
5.1 Information security policy	2.97	3.05	3.28	**3.10**
6.0: Organization of information security				
6.1 Internal Organization	3.59	3.09	3.32	**3.33**
6.2 External Parties	3.21	3.16	3.39	**3.25**
7.0: Asset Management				
7.1 Responsibility for assets	3.30	3.16	3.46	**3.31**
7.2 Information classification	3.13	3.05	3.28	**3.15**
8.0: Human resources security				
8.1 Prior to employment	3.48	3.39	3.49	**3.45**
8.2 During employment	3.08	2.96	3.23	**3.09**
8.3 Termination or change of employment	2.98	2.87	3.14	**3.00**
9.0: Physical and Environmental Security				
9.1 Secure Areas	3.28	3.22	3.43	3.31
9.2 Equipment Security	3.11	3.04	3.25	3.13
10.0: Communications and Operations Management				
10.1 Operational Procedures and responsibilities	3.05	3.12	3.33	**3.17**
10.2 Third party service delivery management	2.78	2.77	3.14	**2.90**
10.3 System planning and acceptance	3.30	3.28	3.45	**3.34**
10.4 Protection against malicious and mobile code	2.97	2.83	3.13	**2.98**
10.5 Backup	3.43	3.40	3.53	**3.45**
10.6 Network Security Management	3.25	3.20	3.30	**3.25**
10.7 Media handling	2.97	3.01	3.16	**3.05**
10.8 Exchange of Information	3.03	2.99	3.19	**3.07**
10.9 Electronic Commerce Services	3.00	3.03	3.27	**3.10**
10.10 Monitoring	3.26	3.22	3.39	**3.29**
11.0: Access Control				
11.1 Business Requirement for Access Control	3.20	3.13	3.37	**3.23**
11.2 User Access Management	3.38	3.34	3.48	**3.40**
11.3 User Responsibilities	3.27	3.27	3.41	**3.32**
11.4 Network Access Control	3.02	3.08	3.31	**3.14**
11.5 Operating system access control	3.27	3.22	3.34	**3.28**
11.6 Application and Information Access Control	3.07	3.08	3.33	**3.16**
11.7 Mobile Computing and teleworking	2.93	2.92	3.10	**2.98**
12.0: Information systems acquisition, development and maintenance				
12.1 Security requirements of information systems	3.00	3.10	3.37	**3.16**
12.2 Correct processing in applications	3.25	3.22	3.28	**3.25**
12.3 Cryptographic controls	3.43	3.38	3.45	**3.42**
12.4 Security of system files	3.18	3.24	3.33	**3.25**
12.5 Security in development and support processes	2.87	2.95	3.18	**3.00**
12.6 Technical Vulnerability Management	2.73	2.80	3.07	**2.87**
13.0: Information security incident management				
13.1 Reporting information security events and weaknesses	3.07	3.15	3.32	**3.18**
13.2 Management of information security incidents and improvements	3.11	3.11	3.26	**3.16**
14.0: Business Continuity Management				
14.1 Information security aspects of business continuity management	3.2	3.22	3.34	**3.25**
15.0: Compliance				
15.1 Compliance with legal requirements	3.30	3.28	3.47	**3.35**
15.2 Compliance with security policies and standards, and technical compliance	3.07	3.00	3.20	**3.09**
15.3 Information Systems audit considerations	3.37	3.38	3.58	**3.44**

.

Table (4): Evaluation Framework Adoption

Item	Organization A	Organization B	Organization C	Total
• **Control Objectives Maturity Level:** $COML_{ji} = \sum_{l=1}^{m}(CIML_{lji} * IC_l)/m$				
$COML_{5.1}$ *(Information security policy)*	2.97	3.05	3.28	**3.10**
$COML_{6.1}$ (Internal Organization)	3.59	3.09	3.32	**3.33**
$COML_{6.2}$ (External Parties)	3.21	3.16	3.39	**3.25**
……				
$COML_{15.3}$ (Information Systems audit considerations)	3.37	3.38	3.58	**3.44**
• **Standard Sections Maturity Level**: $SSML_i = \sum_{j=1}^{n}(COML_{ji} * IS_j)/n$				
$SSML_5$ (Security Policy)	2.97	3.05	3.28	**3.10**
$SSML_6$ (Organization of information security)	3.4	3.12	3.35	**3.29**
$SSML_7$ (Asset Management)	3.22	3.1	3.37	**3.23**
$SSML_8$ (Human resources security)	3.18	3.07	3.29	**3.18**
$SSML_9$ (Physical and Environmental Security)	3.2	3.13	3.34	**3.22**
$SSML_{10}$ (Communications and Operations Management)	3.1	3.09	3.29	**3.16**
$SSML_{11}$ (Access Control)	3.16	3.15	3.34	**3.22**
$SSML_{12}$ (Information systems acquisition, development and maintenance)	3.08	3.12	3.28	**3.16**
$SSML_{13}$ (Information security incident management)	3.09	3.13	3.29	**3.17**
$SSML_{14}$ (Business Continuity Management)	3.2	3.22	3.34	**3.25**
$SSML_{15}$ (Compliance)	3.24	3.22	3.42	**3.29**
• **Organization Security Maturity Level**: $OSML = \sum_{i=1}^{k}((\sum_{j=1}^{n}((\sum_{l=1}^{m}(CIML_{lji} * IC_l)/m) * IS_j)/n) * IO_i)/k$				
$OSML = (SSML_5 + SSML_6 + \ldots + SSML_{15})/11$	3.17	3.13	3.33	**3.21**

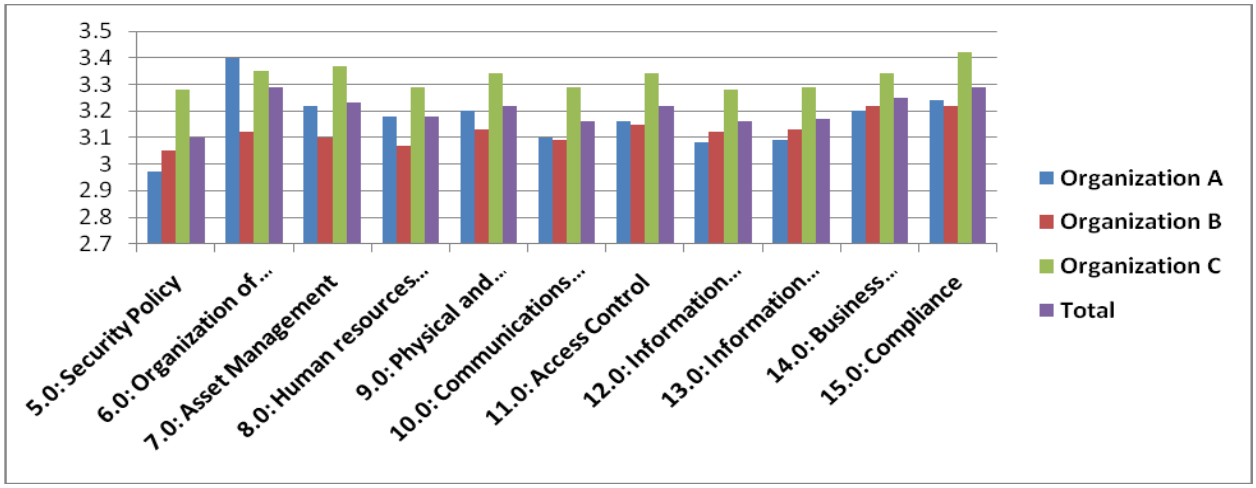

Figure (1): Detailed maturity levels of ISS for the three organizations

REFERENCES

1. Dzazali S., Sulaiman A., and Zolait A., "Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations", *Government Information Quarterly*, Vol. 26, pp. 584–593, 2009.
2. ISO/IEC 17799:2005, "*International Organization for Standardization. Information Technology — Security Techniques — Code of Practice for Information Security Management*", ISO, Geneva, 2005.
3. ISO/IEC 27000:2009, "*Information security management systems — Overview and vocabulary*", ISO, Geneva, 2009.
4. ISO/IEC 27001:2005, "*Information technology - Security techniques — Information security management systems — Requirements*", ISO, Geneva, 2005.
5. ISO/IEC 27002:2005, "*Information technology — Security techniques — Code of practice for information security management*", ISO, Geneva, 2005.
6. ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*", ISO, Geneva, 2005.
7. Karabacak B., and Sogukpinar I., "A quantitative method for ISO 17799 gap analysis", *Computers & Security*, Vol. 25, pp. 413 – 419, 2006.
8. Katsikas S., "Health care management and information system security: awareness, training or education?", *International Journal of Medical Informatics*, Vol. 60, No. 2, pp. 129-135, 2000.
9. Kondakci S., "A new assessment and improvement model of risk propagation in information security", *Int. J. Information and Computer Security*, Vol. 1, No. 3, pp. 341–366, 2007.
10. Lai Y., and Dai R., "The implementation guidance for practicing network isolation by referring to ISO-17799 standard", *Computer Standards & Interfaces*, Vol. 31, pp. 748–756, 2009.
11. NIST, "*An Introduction to Computer Security*", National Institute of Standards and Technology Handbook, Special Publication 800-12, 1995. Accessed: 19-5-2008 from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
12. NIST, "*Information Technology Security Training Requirements: A Role- and Performance-Based Model*", National Institute of Standards and Technology Handbook, special publication 800-16, 1998. Accessed: 19-5-2008 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.
13. NIST, "*Building an Information Technology Security Awareness and Training Program*", National Institute of Standards and Technology Handbook, special publication 800-50, 2003. Accessed: 19-5-2008 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
14. OECD, "*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*", Organization for Economic Co-operation and Development, 2002. Accessed: 7/8/2009 from http://www.oecd.org/dataoecd/16/22/15582260.pdf
15. Peltier T., "*IS security Policies, Procedures, and Standards.*

Guidelines for Effective IS security Management", Auerbach Publications, USA, 2002.

16. René S. "Information Security Management Best Practice Based on ISO/IEC 17799", The Information Management Journal, pp 60-66, 2005.
17. Siponen M., "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", *Information and Organization*, Vol. 15, I. 4, pp. 339-375, 2005.
18. Savola R., and Roning J., "Towards security evaluation based on evidence information collection and impact analysis". *Proceedings of the 2006 international conference on dependable systems and networks (DSN)*, Philadelphia. New York: IEEE Press, pp. 113 - 118, 2006.
19. Solms B., "Information Security governance: COBIT or ISO 17799 or both?", Computers & Security, Vol. 24, pp 99-104, 2005
20. Tudor J., "*IS security Architecture, An Integrated Approach to Security in the Organization*", Auerbach Publications, USA, 2001.
21. Villarroel R., Fernandez-Medina E., and Piattini M., "Secure information systems development – a survey and comparison", *Computers & Security*, Vol. 24, I. 4, pp. 308-321, 2005.
22. Wallace L., Lin H. & Cefaratti M., "Information Security and Sarbanes-Oxley Compliance: An Exploratory Study", *Journal of Information Systems*, Vol. 25, No. 1, pp. 185–211, 2011.
23. Wiander T., "ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners", 18th Australasian Conference on Information Systems, 5-7 Dec 2007, pp 615-621.
24. Yan Q., "A security evaluation approach for information systems in telecommunication enterprises", *Enterprise Information Systems*, Vol. 2, No. 3, pp. 309 - 324, 2008.
25. Yang S., Liu D., and Liu Z., "Evaluating the Network and Information System Security Based on SVM Model", *Journal of Computers*, Vol. 4, No. 11, pp. 1145-1150, 2009.
26. Zaied A., "Priority indexing model for evaluating and analyzing organizations' information security systems", *Int. J. Information Systems and Change Management*, Vol. 4, No. 1, pp. 57 - 65, 2009.http://www.inderscience.com/browse/index.php?journalID=79&year=2009&vol=4&issue=1