Evaluation Framework on System Security Requirements for Government-Owned Agencies in the Philippines

Jonalyn C. Calumpang and Raymund E. Dilan

***Abstract*—This research is mainly focused on the information system security requirements for government-owned agencies in the Philippines. In this research involved determining the evaluation criteria from well-known frameworks, it also involved of limiting the criteria and among these criteria is used to evaluate the information system requirements for government-owned agencies in the Philippines and find which among criteria and frameworks based on result.**

***Index Terms*—Evaluation frameworks, system security requirements, system security.**

I. Introduction

An Overview of Information Security Standards strongly stated that today's rapidly changing technical environment requires government agencies to adopt a minimum set of security controls to protect their information and information system. Information security plays an important role in protecting the assets of an organization. As no single formula can guarantee 100% security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best criteria for security frameworks are adopted. The various standards and regulations that is available for information security, including ISO standards, COBIT, the Sarbanes-Oxley Act, and so on [1]. NIST Special Publication 800-39, stated that organizational risk can include many types of risk (e.g., program management risk, investment risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk). Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their on-going risk management responsibilities [2].

While information security plays an important role in protecting the data and assets of an organization, we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organizations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both governments to address the situation. A number of governments and organizations have set up benchmarks, standards, and in some cases, legal regulations on information security to help ensure an adequate level of security is maintained, resources are used in the right way, and the best security guidelines and frameworks are adopted. Some industries, such as banking, are regulated, and the guidelines or best practices put together as part of those regulations often become a de facto standard among members of these industries [3], [4].

M. Pascucci, if the chosen framework does not cover everything desired, an organization can combine other aspects of different standards to create an initial benchmark. Depending on your industry and your environment, it's going to be hard to find a framework that will fit all your needs perfectly. Using one standard as a benchmark, along with other controls from different benchmarks is completely normal. Administrators have to use their judgment on what they'll enter in their analysis. Many frameworks will work, but it's up to you to make the final call on what the framework ultimately looks like. This is an authoritative starting point, but an organization should still choose its controls appropriately based on its own unique criteria and business objectives [5].

In this paper, we give a brief introduction to the most commonly adopted standards, guidelines or frameworks for information security.

Good security practices can be a force multiplier. By integrating security tasks into job descriptions; installing and updating anti-virus software to local desktops and servers; backing-up important files and storing them in a secure offsite location; insuring processes and procedures are in place; and educating the user population about responsibilities pit falls and time lost by system compromises can be avoided. Although no system connected to the network is 100% secure, your ability to rapidly recover from a compromise can make the difference in the department's productivity.

Information technology and computing pervades every aspect of daily life. Collectively, we use technology to teach and learn, to communicate and collaborate, to manage operations and finances, to access and deliver information and services. However, in this age of dynamic technological change, different channels are prime targets for compromise. Information security experts acknowledge the importance of policies in helping to mitigate liability, reduce costs, cope with regulations and assure proper audit and control procedures for securing our critical infrastructure and assets. Confidentiality, integrity and availability are the three predominant principles of information protection. Compromising these principles leaves systems in jeopardy [6].

With these situations, the researchers aim to conduct a case study on the evaluation framework on information system security requirements for the government-owned agencies in the Philippines. This study sought answers to the problems: 1)

Manuscript received August 15, 2014; revised December 1, 2014.

Jonalyn C. Calumpang is with College of Computer Studies and Engineering and Don Mariano Marcos Memorial State University-Mid La Union Campus, Philippines (e-mail: jonac_calumps@yahoo.com.ph).

Raymund E. Dilan is with University of the Cordilleras, Philippines.

what are the criteria in evaluating information system security requirements? And 2) what are the evaluation criteria for Philippines information system security requirements?

II. Methods

The researcher used descriptive type of research to organize the presentation, prescription, and interpretation of data gathered.

TABLE I: The Government Owned Agencies (Philippines)

Government Owned Agencies in the Philippines	
1.GSIS	Government Service Insurance System
2.Pag-ibig	Pag-Ibig Fund, For Home Development Mutual Fund
3.Phil health	Philippine Health Insurance
4.BIR	Bureau Internal Revenue
5.DOLE	Department of Labour and Employment
6.POEA	Philippine Overseas Employment Administration
7.DOST	Department of Science and Technology
8.NEDA	National Economic and Development Authority
9.BFAR	Bureau of Fisheries and Aquatic Resources
10.DSWD	Department of Social Welfare and Development
11.CHED	Commission on Higher Education of the Philippines

Descriptive research according to Calmorin (2005) as cited by Valdez (2009), involves the description, recording, analysis, and interpretation of present nature, composition or processes of phenomena. It goes beyond mere gathering and tabulation of data for it involves the elements or interpretation of the meaning and significance of what is described, thus it becomes a basis to develop a new concept.

This study was conducted at San Fernando City, La Union. The respondents were the MIS or head of government owned-agencies specifically Region I. The agencies are located below Table I.

A. Instruments

In order to address the objectives of the study, the researcher used survey as data collection method.

B. Categorization of Data

The gathered data were interpreted using the five-point Likert scale presented in Table II: (WAMMI and SAUMUR)

TABLE II: Level of Security in Terms of Criteria

Scale	Mean	Descriptive rating	Overall descriptive
5	4.20-5.00	Strongly implemented	Very high
4	3.40-4.19	Moderately implemented	High
3	2.60-3.39	Neutrally implemented	Moderate
2	1.80-2.59	Partially implemented	Fair
1	1.00-1.79	Not Implemented	Poor

C. Collection of Frameworks and Criteria

The collections of different frameworks were collected and tabulated to select the criteria; this criterion was used for the survey of the government-owned agencies. The collected data are presented in Table III.

TABLE III: Collections of Frameworks and Criteria

FRAME WORKS	CRITERIA								
	Minimal Protection security requirements [14]	Discretionary protection [14]	Mandatory protection [14]	Verified protection [14]	Functional security requirements	Measures security requirements	Information security requirements	Managed information security	Customer security
1.DDS	✓	✓	✓	✓					
2. (CC)					✓	✓	✓		
3.NIST	✓								
4.COBIT					✓	✓			
5.PCIDS					✓	✓	✓		
6. ISF							✓		
7.ISO/IEC 27001:2005(en)				✓	✓	✓	✓	✓	
8.HIPPPA							✓	✓	✓
Total	2	1	1	2	4	4	5	2	1

1) Department of defense trusted computer system evaluation criteria

Minimal Protection. This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

Discretionary Protection. Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.

Mandatory Protection. The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Verified Protection. This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation [7].

2) ISO/IEC 15408 (evaluation criteria for IT security)

The international standard ISO/IEC 15408 is commonly known as the "Common Criteria" (CC) 12. It consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements) and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard [8].

3) Institute of standards and technology (NIST)

It is an official series of publications relating to standards and guidelines adopted and made available under the provisions of the FISMA , FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, is the first mandatory security standard laid down under the FISMA legislation. FIPS Publication 200, entitled "Minimum Security Requirements for Federal Information and Information Systems" is the second mandatory set of security standards that specify minimum security requirements for US federal information and information systems across 17 security-related areas. US federal agencies must meet the minimum security requirements defined in this standard by selecting appropriate security controls and assurance requirements laid down in NIST Special Publication 800-53. The 17 security-related areas include: a) access control; b) awareness and training; c) audit and accountability; d) certification, accreditation, and security assessments; e) configuration management; f) contingency planning; g) identification and authentication; h) incident response; i) maintenance; j) media protection; k) physical and environmental protection; l) planning; m) personnel security; n) risk assessment; o) systems and services acquisition; p) system and communications protection; and q) system and information integrity [9].

4) COBIT

The Control Objectives for Information and related Technology (COBIT) is "a control framework that links IT initiatives to business requirements organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged [10].

5) Payment card industry data security standard

The Payment Card Industry (PCI) Data Security Standard (DSS) 16 was developed by a number of major credit card companies (including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) as members of the PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measure [11].

6) Information security forum (ISF) standard of good practice

The ISF has developed a security model to support organizations in designing their approach to addressing information security and to give them a basis for identifying the key aspects of an information security programme. The ISF provides insights, best practice standards and tools which address each aspect of the model to aid organizations in enhancing their information security environment [12].

7) ISO/IEC 27001: 2005 (information security management system-requirements)

The international standard ISO/IEC 27001:2005 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organization. It is 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, including business enterprises, government agencies, and so on [13].

8) HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a US law designed to improve the portability and continuity of health insurance coverage in both the group and individual markets, and to combat waste, fraud, and abuse in health insurance and health care delivery as well as other purposes. The Act defines security standards for healthcare information, and it takes into account a number of factors including the technical capabilities of record systems used to maintain health information, the cost of security measures, the need for training personnel, the value of audit trails in computerized record systems, and the needs and capabilities of small healthcare providers [14].

III. Review of Related Literature

The advent of the Internet is changing the manner in which business is being conducted around the world. This Internet-driven world, as a direct influence on the increasing reliance on information technology (IT), necessitates well implemented and comprehensive security mechanisms in products and systems alike [15].

Fundamental security issues such as authentication, encryption, and protection of data, user privileges, and audit and network security still occupy center stage in such a dynamic computing environment, but so do innovations in IT security fraud [16].

The problem of insecure software is perhaps the most important technical challenge of our time. Security is now the key limiting factor on what we are able to create with information technology. At The Open Web Application Security Project (OWASP), we're trying to make the world a place where insecure software is the anomaly, not the norm, and the OWASP Testing Guide is an important piece of the puzzle. It goes without saying that you can't build a secure application without performing security testing on it. Yet many software development organizations do not include security testing as part of their standard software development process. Still, security testing, by itself, isn't a particularly good measure of how secure an application is, because there are an infinite number of ways that an attacker might be able to make an application break, and it simply isn't possible to test them all [17].

However, security testing has the unique power to absolutely convince naysayers that there is a problem. So

security testing has proven itself as a key ingredient in any organization that needs to trust the software it produces or uses [18].

Security evaluations by independent organizations provide assurance in the security of Information Technology (IT) products and systems to commercial, government, and military institutions. The growth of the Internet and Electronic Commerce, as a direct influence on the increasing reliance on IT, necessitates independent security evaluations to provide an accurate assessment of the strength of security mechanisms in IT products and systems. Such evaluations and the criteria upon which they are based serve to establish an acceptable level of confidence for IT purchasers and vendors alike. Furthermore, security evaluation criteria and ratings can be used as concise expressions of IT security requirements [19].

There are two important components of IT security evaluations: The criteria, against which the evaluations are performed, and the schemes or methodologies which govern how and by whom such evaluations can be officially performed [20].

Systems Security Engineering-Capability Maturity Model (SSE-CMM) is a process reference model created for security system development process. It provides a framework to measure and improve performances in the application of security engineering principles. Same as Capability Maturity Model (CMM), SSE-CMM has five capability levels: Capability level 1 - performed informally; capability level 2 - planned and tracked; capability level 3 - well defined; capability level 4 - quantitatively controlled; capability level 5 - continuously improving [21].

IV. Results and Discussions

The following information describes the level of security of the Evaluation Framework on System Security Requirements for Government-owned Agencies in the Philippines.

The Evaluation Framework on System Security Requirements for Government-owned Agencies in the Philippines, was evaluated for its level of security in terms of criteria and among these are functional security requirements, measures security requirements, information security requirements, minimal protection/security requirements, verified protection, and managed information security by GSIS, Pag-ibig, Phil health, BIR, DOLE, POEA, DOST, NEDA, BFAR, DSWD, and CHED.

TABLE IV: Level of Security in Terms of Criteria

CRITERIA	Functional security requirements	Measures security requirements	Information security requirements	Minimal protection	Verified protection	Managed information security	Mean rating
1. GSIS	5	5	5	5	5	5	5.00
2. Pag-ibig	5	5	5	5	5	5	5.00
3. PhilHealth	5	5	5	5	5	5	5.00
4. BIR	5	5	5	5	5	5	5.00
5. DOLE	2	1	3	5	3	2	2.67
6. POEA	3	1	3	5	3	2	2.83
7. DOST	3	1	3	5	3	2	2..83
8. NEDA	5	5	5	5	5	5	5.00
9. BFAR	2	1	1	5	3	2	2.33
10. DSWD	2	1	1	5	3	2	2.33
11. CHED	1	1	1	5	3	2	2.20
Overall Mean	3.45	2.82	3.18	5.00	3.91	3.36	3.62
DER	HIGH	MODERATE	MODERATE	VERY HIGH	HIGH	MODERATE	HIGH

Table IV shows the level of security in terms of criteria. It can be noted that the level of security in terms of minimum security/ protection requirements is very high as evidenced by the mean rating of 5.00. The indicator described as strongly implemented in all areas. Under this minimum security/protection criteria contained security related areas. Which means that the government of the Philippines have These seventeen (17) security-related areas include: a) access control; b) awareness and training; c) audit and accountability; d) certification, accreditation, and security assessments; e) configuration management; f) contingency planning; g) identification and authentication; h) incident response; i) maintenance; j) media protection; k) physical and environmental protection; l) planning; m) personnel security; n) risk assessment; o) systems and services acquisition; p) system and communications protection; and q) system and information integrity. Along with "Minimum Security Requirements for Federal Information and Information Systems" is the second mandatory set of security standards that specify minimum security requirements for US federal information and information systems across 17 security-related areas. US federal agencies must meet the minimum security requirements defined in this standard by selecting appropriate security controls and assurance requirements laid down in NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems) [22].

Functional security requirements and verified protection are high as evidenced by the mean rating of 3.45 and 3.91. The indicator describe moderately implemented in the area of GSIS, Pag-ibig, Philhealth, BIR and NEDA they got the highest rating with the mean of 5.00 and followed by the DOST, DOLE, POEA, DOST, BFAR, DSWD and POEA with the mean rating of 3.00 which is indicates neutrally

implemented and CHED got the lowest rating although it described overall rating as high. Based on the overall result it is obviously means that the level of security in terms of functional security requirements and verified protection are the criterion that is used for the Philippines information system security requirements.

It is worthy to note also that the measures security requirements, information security requirements and managed information security other owned agencies gave a moderate rating as reflected in the mean of 2.82 , 3.18, 3.36 this means that the level of security is neutrally implemented.

Although there are a number of standards on information security available now, these standards are often general guidelines or principles that may not all be applicable to a particular organization. If an organization aims to implement security controls that are in compliance with a particular standard, or even a set of standards, a concerted effort from top management down to end-users would be required as part of the development and implementation process. Care must be taken to ensure that standardized policies or guidelines are applicable to, and practical for, that particular organization's culture, business and operational practices.

The organization should first perform a "gap analysis" to identify the current security controls within the organization, the potential problems and issues, the costs and benefits, the operational impact, and the proposed recommendations before applying any chosen standards. The creation of security policies and guidelines should only follow the completion of a gap analysis. Management support is necessary at all levels. User awareness programmers should also be conducted to ensure that all employees understand the benefits and impacts before the deployment of new security policies and guidelines.

A common problem that crops up after implementation of a standardization exercise is an increase in the number of complaints received from users of IT services due to the restrictions imposed by new security controls. The successful implementation of any information security standards or controls must be a balance of security requirements, functional requirements and user requirements.

V. Conclusion

Evaluation Framework on System Security Requirements for Government-owned Agencies in the Philippines was conducted to determine the criteria in evaluating information system security requirements and also to determine the evaluation criteria for the Philippines information system security requirements. The plan for the study serves as the basis of the level of security in terms of criteria and the criteria are helpful for the conducted study. The collections of different frameworks were collected and tabulated to get the criteria that are used for the survey of the owned government agencies in San Fernando City La Union.

The study is able to limit criteria in evaluating information system security requirements and the criteria are Functional security requirements, Measures security requirements, Information security requirements, Minimal protection/security requirements, Verified protection, and Managed information security.

The evaluation criteria for Philippines information system security requirements was Minimal protection/the minimum security requirements which consists of 17 security-related areas.

Although there are a number of information security standards available, an organization can only benefit if those standards are implemented properly. Security is something that all parties should be involved in. Top managements and user's all have a role to play in securing the assets of an organization. It can only be success of information security if there are a full cooperation at all levels of an organization.

Acknowledgment

The first author would like to thank all the people who, in one way or another, have helped me in making this research possible most especially to my parents, family Mar my husband, Joshua my son and Xamwellen my daughter, as well as to my Auntie's Erlinda, Imelda, Marcy, Revie, and Uncle Francis for your unconditional love and support.

References

[1] An overview of information security standards-summary. (Feb. 18, 2008). The Government of the Hong Kong Special Administrative. [Online]. Available: http://www.infosec.gov.hk/english/technical/files/overview.pdf
[2] J. U. Duncombe, "Infrared navigation — Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34-39, Jan. 1959.
[3] Network world. [Online]. Available: http://www.networkworld.com/news/2006/030706-government-cio-survey.html
[4] Deloitte. [Online]. Available: http://www.deloitte.com/dtt/press_release/0,1014,sid%253D1000%252 6cid%253D171269,00.html
[5] M. Pascucci. Key steps to perform a successful information security gap analysis. [Online]. Available: http://searchsecurity.techtarget.com/tip/Key-steps-to-perform-a-successful-information-security-gap-analysis
[6] *Information Protection and Security*, Rutgers of Office Information Technology.
[7] D. C. Latham, "Trusted computer system evaluation criteria," Department of Defense Standard.
[8] Common Criteria Project Sponsoring Organizations, "Common criteria for information technology security evaluation, part 1: Introduction and general model," *CCIMB*, January 2004.
[9] National Institute of Standards and Technology, "Minimum security requirements for federal information and information systems," *FIPS PUB 200*, March 2006.
[10] IT Governance Institute, "COBIT 4.0.," USA, 2005.
[11] J. Eloff and M. Eloff, "Information security management," in *Proc. SAICSIT 2003*, 2003, pp. 130-136.
[12] Information Security Forum, "The standard of good practice for information security," 2005.
[13] International Organization for Standardization, "ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements," June 2005.
[14] National Institute of Standards and Technology, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, NIST Special Publication 800-27, June 2004.
[15] J. S. Tiller, *The Ethical Hack: A Framework for Business Value Penetration Testing*, Auerbach Publications, 2004.
[16] S. Young and D. Aitel, *The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks*, Auerbach Publications, 2003.
[17] M. Graff and K. V. Wyk, *Secure Coding*, O'Reilly, 2003.
[18] S. Huseby, *Innocent Code: A Security Wake-up Call for Web Programmers*, John Wiley & Sons, 2004.
[19] G. McGraw and G. Hoglund, *Exploiting Software: How to Break Code*, Addison-Wesley Pub Co., 2004.
[20] S. Robertson and J. Robertsonn, *Mastering the Requirements Process*, Addison-Wesley Professional, 2012.

[21] J. Scambray and M. Shema, *Web Applications (Hacking Exposed)*, McGraw-Hill Osborne Media, 2002.
[22] National Institute of Standards and Technology, *Information Security Handbook: A Guide for Managers*, NIST Special Publication 800-100, October 2006.

Jonalyn C. Calumpang was born in San Francisco San Fernando, La Union on July 29, 1979. She got her bachelor of science in computer science at STI College, Philippines, 2009 and the master of arts in science education minor in Technological Vocational School Management at Don Mariano Marcos Memorial State University, Philippines, 2012.

She was first employed by La Union Cultural Institute as a high school and elementary teacher. Then she was employed at Lorma Colleges at the College of Computer Studies and Engineering and Don Mariano Marcos Memorial State University-Mid La Union Campus at the College of Arts and Sciences as a computer instructor.

Mrs. Calumpang is affiliated with the Philippine e-Learning Society Incorporated, Association of the Philippine College of Arts and Sciences-Region I, NAKEM Conferences International-Philippines Chapter. She was awarded as the coach of the first place winner of STEP Division skills Development and Competition. She got the certificate of recognition as a finalist during the search for the best thesis/dissertation and for scholarly performance on her research entitled e-journal for master of arts in science education (MASE) researches and certificate of recognition for successful student leadership.

Raymund E. Dilan was born in Baguio City, Philippines on July 26, 1972. He got his bachelor of science in computer and information science at Baguio College Foundation, Philippines, and the master of computer science at De La Salle University, Philippines.

He was first employed at University of Baguio as a primary, secondary and undergraduate Program teacher. Then he was employed at University of the Cordilleras for undergraduate and graduate programs.

Mr. Dilan is affiliated with the Philippine Society of Information Technology Educators (PSITE) Chapter Member Council – PSITE-Northern Luzon 1 Chapter, and Philippine Computing Society. He was awarded as Cum Laude for undergraduate degree bachelor of science in computer and information science.