Maturity Level of Information Systems Security and Control: A Survey of Companies in Thailand

Chamaiporn Theerakarn
Metropolitan Waterworks Authority

Nitaya Wongpinunwatana
Thammasat University

Thunyanee Pothisarn
NIDA

The objective of this study is to survey companies' information systems security and control, and to develop a maturity level of information systems security and control application. This application shows a company's position of information systems security and control by comparing this position with other companies. This study is survey research. Participants are chief information security officers of 304 Stock Exchange of Thailand listed companies within eight industry groups (services, property and construction, industrials, financials, agriculture and food industry, consumer products, technology, and natural resources). The findings suggest that all companies are aware of security of network access control. Many companies also implement information security policies, asset management systems, and access controls for data, information systems and business applications.

INTRODUCTION

Recently, information systems (IS) security and control has shown itself to be an important issue in both the private and government sectors. Many businesses still are not properly protected or are unprepared for a variety of IS threats (EYGM Limited, 2013). The information security threats, which are events that damage computer resources, have affected many societies that utilize computers. Microsoft Corporation reported that five million personal computers around the world were used illicitly to steal money from dozens of financial institutions. Other examples of recent threats include Facebook breaches, and ATM malware that forced them to illicitly dispense banknotes (Charoenkiatpakul, 2016; Nieva et al., 2018).

The Thailand Computer Emergency Response Team (ThaiCert) reported a total of 10,590 cases of computer threats in Thailand during the period of January 2014 to June 2016 (ThaiCert, 2017). This report presented three common complaints: fraud, malicious codes, and intrusions. Moreover, surveys on the IS threats to companies listed on the Stock Exchange of Thailand reported that the top three most

likely threats are viruses, malware, and access to systems by hackers (Sumtumthip and Wongpinunwatana, 2017).

Therefore, organizations need to implement IS security and control to reduce security threats. In addition, comparing IS security and control of one organization with others will provide more benefit to the organization. The main goal of this research is to build initial tools that companies can use to compare their information security control with other companies. In other words, the companies will be able to identify what is an adequate level of IS security and control, and compare their maturity level of IS security and control with other companies.

INFORMATION SYSTEMS SECURITY AND CONTROL FRAMEWORKS

Many organizations, both in the private and government sectors, have utilized standard models for implementing IS security and control (Susanto et al., 2011). Standards provide high levels of quality, safety, reliability, efficiency and interchangeability for products and services (Tofan, 2011). Moreover, standards can be used to compare the level of IS security and control of an organization with other organizations (Tofan, 2011). The commonly used IS security and control frameworks are the Control Objectives for Information and related Technology (COBIT), Committee of Sponsoring Organizations of the Treadway Commission (COSO), Information Technology Infrastructure Library (ITIL), and ISO27001:2013 (Pedersen & Bjørn-Andersen, 2011; ISACA, 2012; Sheikhpour & Modiri, 2012; ITIL, 2013; Peña et al., 2013).

COBIT is a framework to provide management with information technology (IT) governance in order to control and manage IT (Sheikhpour & Modiri, 2012). COBIT identified five IT governance domains: strategy alignment, value delivery, resource management, risk management and performance measurement (Susanto, 2011). Sheikhpour and Modiri (2012) noted that information management and controls are the important keys of the COBIT framework in ensuring alignment to business needs. Thus, the main focus of COBIT is on the IT process.

COSO is a framework to assist organizations regarding (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations. COSO places more emphasis on general control, more so than other frameworks.

ITIL has become well known for its concepts and practices related to IT services management, development, and operation, which are all integral parts of security (Susanto, 2011). The goals of ITIL are to transform IT departments into service-oriented organizations (Pentildéa, et al, 2013). ITIL has been widely adopted to properly manage and improve IT services in organizations. This has been accomplished, for example, by building and maintaining positive business relationships with customers, thereby improving customer satisfaction (Al-Ahmad & Mohammad, 2012). Clinch (2009) stated that ITIL has contributed to key benefits obtained by organizations by deploying the techniques and procedures throughout their organizations. Thus, ITIL can be used as a basis for IT service level agreements.

ISO27001:2013 is the best-known standard that helps organizations keep information resources secure. The purpose of ISO27001:2013 is to provide an approach for the management of information security within an organization. Magalhaes (2013) identified the benefits of ISO27001:2013 as: ability to demonstrate security, ability to identify the requirements of regulatory and compliance, ability to preserve highly confidential information, ability to transfer information securely, ability to improve competitive advantage, ability to reduce and manage risks, ability to save costs, ability to deliver products and services consistently, and ability to protect resources/shareholders/directors in an organization. ISO27001:2013 has been adopted by many organizations for establishing, implementing, operating, monitoring, and maintaining IS security management (Sharma & Dash, 2012; Magalhaes, 2013).

Twenty-seven essential questions used to measure formulation or enforcement of companies' IS security and control were derived from Annex A of ISO27001:2013 (see Table 1). These questions cover measurement of IS security and control which should be implemented by organizations, as suggested by Kanno (2008).

TABLE 1
MAPPING CLAUSE TITLE WTH MEASUREMENT QUESTIONS

Clause titles from ISO27001:2013 Annex A	Measurement questions for formulation of IS security and control
1. Organizational approaches to information security:	
- Information security policies - Organization of information security - Human resources security - Asset management - Supplier relationships - Compliance	- Information security policies - Mobile devices and teleworking handling - Risk assessment - Regulation of prior, during, termination, and change of employment - Training on IS security and control for staff - Information classification - Responsibility for assets - Media handling - Supplier service delivery management - Compliance with legal and contractual requirements
2. Physical environmental security countermeasures:	
- Physical and environmental security - Operations security	- Secure areas and equipment - Operational procedures and responsibilities for secure areas - Backup - Protection from malware - Technical vulnerability management - Control of operational software - Logging and monitoring
3. Operation and maintenance controls over IS and communication networks:	
- Cryptography - Communications security	- Network security management - Protection on information transfer
4. IS access control, security countermeasures for the development and maintenance phases:	
- Access control - Systems acquisition, development and maintenance	- Access control for data, information systems and business applications - User access management and responsibilities - Network access control - Security requirements of information systems - Security in development and support processes
5. Information security incident response and business continuity management:	
- Information security incident management - Information security aspects of business continuity management	- Management of information security incidents and improvements - Business continuity - Management system failure

METHOD

Information security and control questionnaires were sent to 476 companies listed on the Stock Exchange of Thailand. These companies are in eight industry groups (services, property and construction, industrials, financials, agriculture and food industry, consumer products, technology, and natural resources). The participants who completed the questionnaire are chief information security officers. In the questionnaire, participants gave their answers using a five-point Likert scale. The scale ranges from 1

for "strongly disagree" to 5 for "strongly agree" – a higher score indicates stronger agreement. A five-point Likert scale was used to rate the 27 essential questions in Table 1 which measured companies' IS security and control.

RESULTS

Analysis of Results

In total, 304 companies completed questionnaires. The average score of each item for each company was calculated. The ideal score as suggested by Kanno (2008) also was calculated, which indicates the average score of the top 1/3 organizations in a group. In other words, the ideal score is the IS security and control that a company in the group should implement. In addition, the average score of each item was also grouped by medium-size and large-size companies.

Table 2 displays the average score of IS security and control for all companies. The average scores are also grouped by size of company: medium size and large size. Detailed analysis of Table 2 indicates that (1) access control for data, information systems and business applications and (2) network access control are the two most concerning items for IS security and control in medium-size organizations. On the other hand, large-size organizations are more concerned with information security policy, responsibility of assets and network access control.

TABLE 2
AVERAGE SCORE OF IS SECURITY AND CONTROL FOR MEDIUM AND LARGE-SIZE COMPANIES

No	Title	Average score of IS security and control	
		Medium size	Large size
1	Information security policies	3.47	**3.99**
2	Risk assessment	3.18	3.65
3	Responsibility for assets	3.41	**3.99**
4	Information classification	3.24	3.70
5	Mobile devices and teleworking handling	3.32	3.62
6	Supplier service delivery management	3.20	3.69
7	Regulation of prior, during, termination and change of employment	3.32	3.54
8	Training on IS security and control for staff	2.99	3.16
9	Compliance with legal and contractual requirements	3.21	3.68
10	Logging and monitoring	3.33	3.8
11	Control of operational software	3.34	3.62
12	Media handling	3.28	3.49
13	Secure areas and equipment	3.23	3.56
14	Operational procedures and responsibilities for secure areas	3.21	3.73
15	Backup	3.38	3.66
16	Protection from malware	3.29	3.78
17	Technical vulnerability management	3.05	3.45
18	Network security management	3.37	3.84
19	Protection on information transfer	2.82	3.21
20	User access management and responsibilities	3.50	3.85

TABLE 2
AVERAGE SCORE OF IS SECURITY AND CONTROL FOR MEDIUM AND LARGE-SIZE COMPANIES (CONTINUED)

No	Title	Average score of IS security and control	
		Medium size	Large size
21	Access control for data, information systems, and business applications	**3.54**	3.86
22	Network access control	**3.53**	**4.03**
23	Security in development and support processes	3.21	3.57
24	Security requirements of information systems	3.38	3.83
25	Management system failure	3.25	3.66
26	Management of information security incidents and improvements	3.17	3.54
27	Business continuity	3.09	3.60
Total		**3.28**	**3.67**

Figure 1 is a radar chart providing information on IS security and control from the 27 measurement questions. The companies' average score is shown in the inner ring (plain line), and the ideal level is shown in the outer ring (bold line). The chart shows that all companies are aware of security of network access control. The results of all companies in the radar chart are summarized in Table 3. This research also calculated the average score and ideal level of information security and control by industry group. Thus, a company will know its position of IS security and control by comparing its IS security and control with companies within the same industry group. The company also will know its position of IS security and control compared to all surveyed companies.

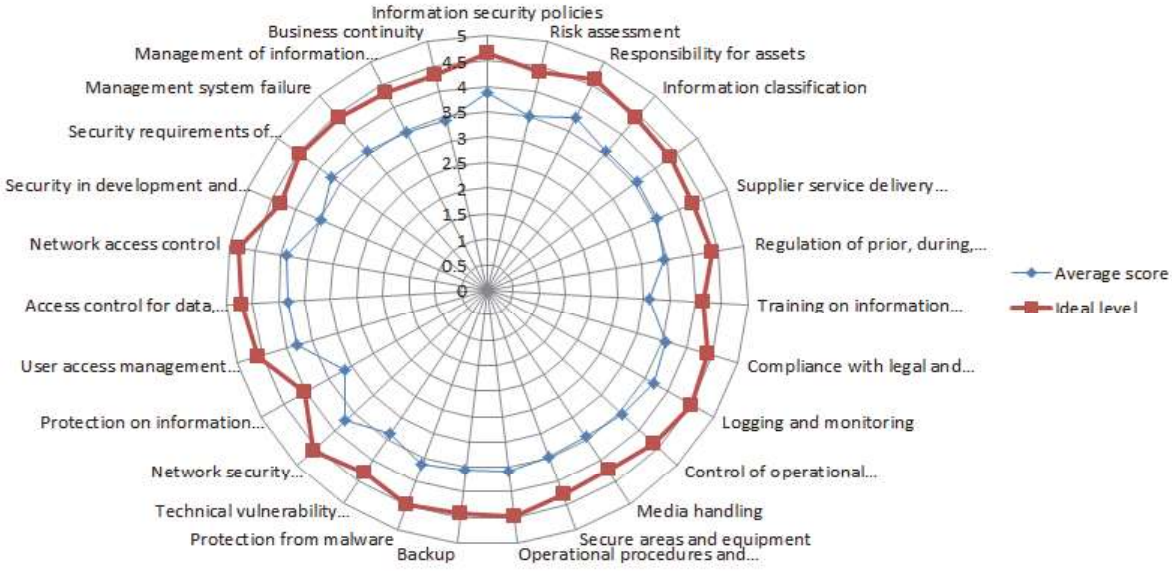
TABLE 3
AVERAGE SCORE AND IDEAL LEVEL OF IS SECURITY AND CONTROL FOR ALL COMPANIES

No	Title	Average score	Ideal level
1	Information security policies	3.88	4.66
2	Risk assessment	3.52	4.38
3	Responsibility for assets	3.79	4.63
4	Information classification	3.54	4.43
5	Mobile devices and teleworking handling	3.57	4.39
6	Supplier service delivery management	3.54	4.28
7	Regulation of prior, during, termination and change of employment	3.44	4.37
8	Training on IS security and control for staff	3.11	4.14
9	Compliance with legal and contractual requirements	3.57	4.40
10	Logging and monitoring	3.68	4.52
11	Control of operational software	3.56	4.38
12	Media handling	3.44	4.24
13	Secure areas and equipment	3.48	4.26
14	Operational procedures and responsibilities for secure areas	3.58	4.49

TABLE 3
AVERAGE SCORE AND IDEAL LEVEL OF IS SECURITY AND CONTROL FOR ALL COMPANIES (CONTINUED)

No	Title	Average score	Ideal level
15	Backup	3.54	4.42
16	Protection from malware	3.64	4.50
17	Technical vulnerability management	3.36	4.29
18	Network security management	3.73	4.58
19	Protection on information transfer	3.14	4.03
20	User access management and responsibilities	3.81	4.58
21	Access control for data, information systems, and business applications	3.81	4.71
22	Network access control	3.90	**4.83**
23	Security in development and support processes	3.45	4.29
24	Security requirements of information systems	3.72	4.46
25	Management system failure	3.54	4.42
26	Management of information security incidents and improvements	3.46	4.33
27	Business continuity	3.42	4.33
Total		**3.57**	**4.42**

FIGURE 1
RADAR CHART OF AVERAGE SCORE AND IDEAL LEVEL OF IS SECURITY AND CONTROL FOR ALL COMPANIES

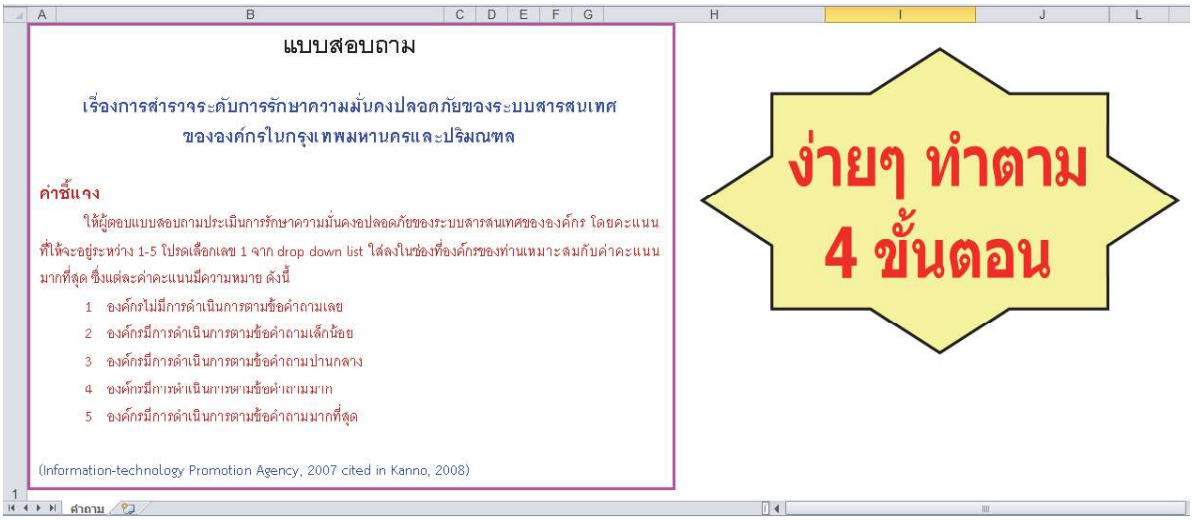


In summary, the average score and ideal level of IS security and control show that all companies in eight industry groups give priority to information security policy and network access control.

Construction of Application

Excel Visual Basic for Applications (VBA) was used to develop the Maturity Level of IS Security and Control application (MLISSC). The interface screens of this application start with the main menu as shown in Figure 2. This menu explains how to respond to the measurement questions by using the five-point Likert scale. The screen also indicates the four steps to get to the maturity results.

FIGURE 2
MAIN MENU



Step 1: Company fills in the rating scale for each measurement question. After the rating scale has been entered, the application calculates IS security and control for each question as shown in Figure 3.

FIGURE 3
MEASUREMENT QUESTIONS

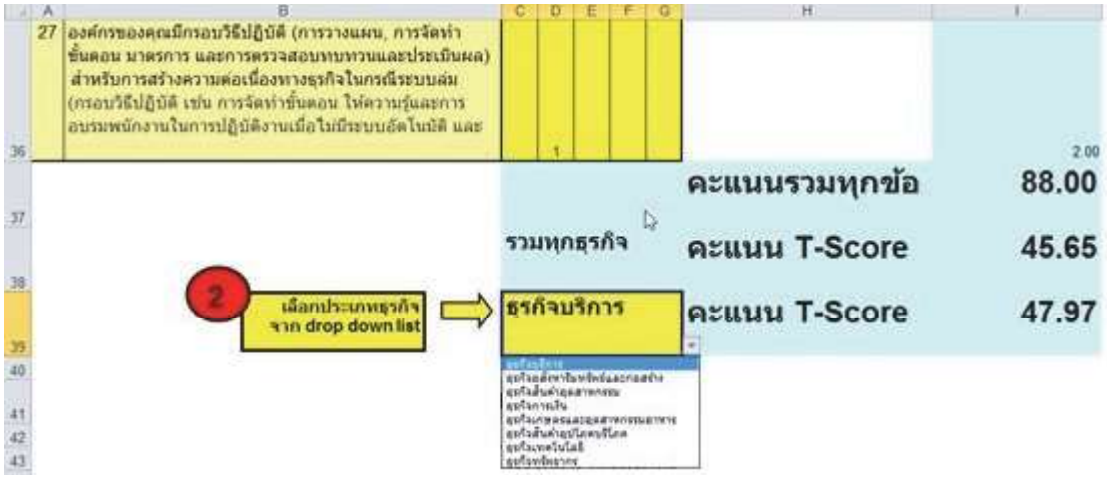
ข้อที่	คำถาม	การดำเนินการตาม					
		ไม่มี	น้อย	ปานก	มาก	มากที่	
		1	2	3	4	5	
เรื่องที่ 1 แนวทางขององค์กรในการรักษาความมั่นคง							คะแนนแต่ละข้อ
1	องค์กรของคุณมีนโยบายหรือระเบียบข้อบังคับในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และมีการบังคับใช้จริง			1			3.00
2	องค์กรของคุณมีการประเมินอันตรายและช่องโหว่ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของทรัพย์สินสำคัญที่เกี่ยวข้องกับสารสนเทศ (เช่น ข้อมูล, อีเมล, handy drive เป็นต้น)			1			3.00
3	องค์กรของคุณมีการบริหารจัดการเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (เช่น การจัดโครงสร้างองค์กร แบ่งแยกหน้าที่งาน และควบคุมการดำเนินงาน เป็นต้น) และดำเนินการสอดคล้องกับกฎหมายและระเบียบข้อบังคับขององค์กร			1			3.00
4	องค์กรของคุณมีการแบ่งระดับชั้นความสำคัญและแบ่งระดับชั้นความลับของทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ (เช่น ข้อมูล, อีเมล, handy drive เป็นต้น)					1	5.00
5	องค์กรของคุณมีการบริหารจัดการทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ (เช่น ข้อมูล, อีเมล, handy drive) อย่าง						

1 เลือกจาก drop down list

Step 2: After the user answers the measurement questions by completing the rating scales, the application calculates the IS security and control score and shows the total score of the company, and the

T-score of all companies and selected industry groups that completed the questionnaires, as shown in Figure 4.

FIGURE 4
TOTAL SCORE OF IS SECURITY AND CONTROL



Steps 3 and 4: The application shows the maturity level of IS security and control in a radar chart. This chart compares the IS security and control score of the company with all companies and with the ideal level as shown in Figure 5. In addition, the application also calculates the standardized score of IS security and control and shows it in the form of a bar chart as shown in Figure 6. Additionally, the company can select industry group in Step 2 to compare its IS security and control with other companies within the same industry group.

FIGURE 5
RADAR CHART OF MATURITY LEVEL OF IS SECURITY AND CONTROL

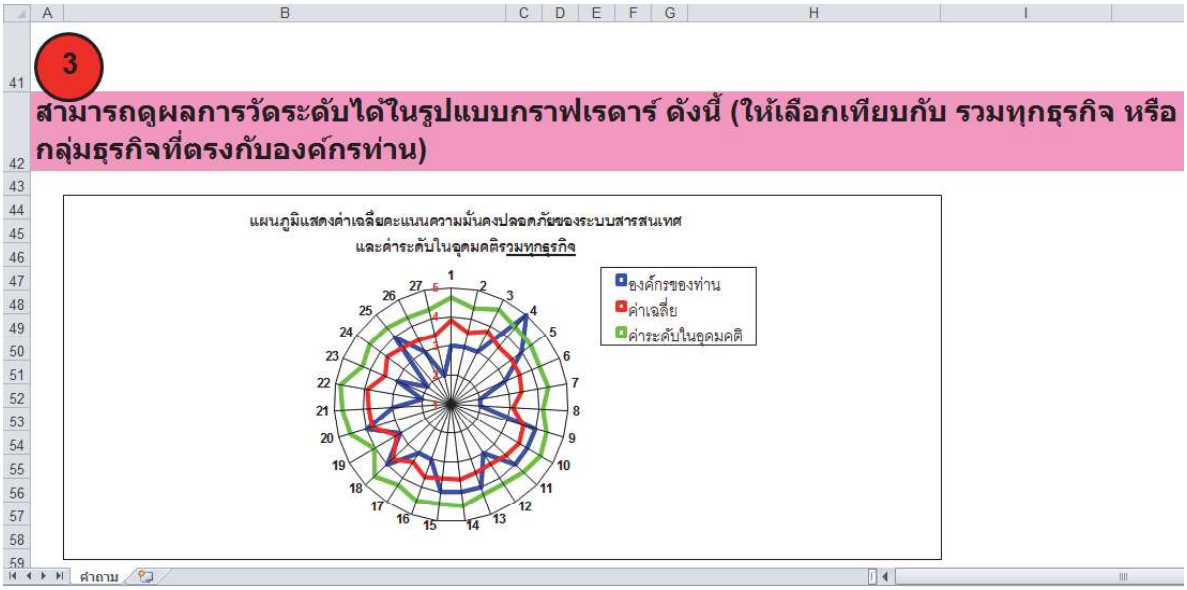
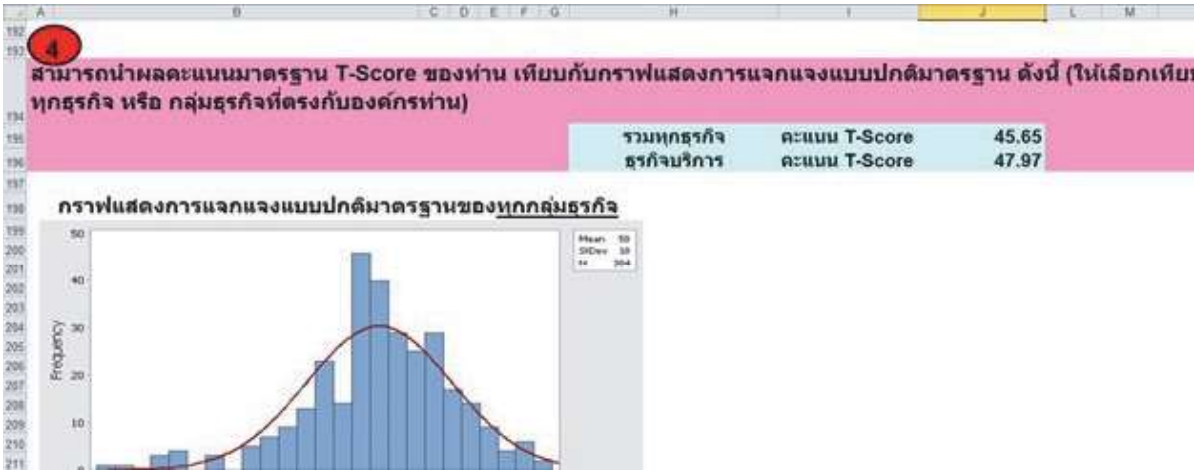


FIGURE 6
BAR CHART OF STANDARDIZED SCORE OF IS SECURITY AND CONTROL



CONCLUSION

This research surveyed IS security and control of companies in the Bangkok, Thailand metropolitan area based on ISO27001: 2013. The Maturity Level of IS Security and Control application (MLISSC) was developed based on collected data from the survey. This survey reveals that most companies are aware of implementing information security policies and network access control. Different industry groups and company sizes may emphasize different areas of IS security and control; however, almost all companies are aware of network access and control.

This study will help companies assess their maturity level of IS security and control and compare it to other companies. The results will be useful for governments to promote awareness of IS security and control because computer threats affect confidentiality, integrity, and continuity of companies.

This research collected IS security and control based on IS27001:2013 Annex A. There are other IS security and control frameworks such as COBIT and COSO, and future research may collect data based on these other frameworks. In addition, future research may utilize in-depth interviews to get detailed information on IS security and control and examine reasons why some companies do not implement IS security and control.

REFERENCES

Al-Ahmad, W., & Mohammad, B. (2012). Can A Single Security Framework Address Information Security Risks Adequately? *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 2(3), 222-230.

Charoenkiatpakul, W. (2016, August 24). Manhunt for ATM robbers kicks off. Bangkokpost, 1.

Clinch, J. (2009). ITIL V3 and Information Security. Retrieved December 31, 2013, from http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf.

EYGM Limited (2013). EY's Global Information Security Survey 2013. Retrieved Jan 2, 2014, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/ assets/2013-giss-report.pdf.

ISACA (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Retrieved Jan 2, 2014 from, http://www.isaca.org/COBIT/Pages/ default.aspx.

ITIL (2013). *What is ITIL?* Retrieved October 31, 2013, from http://www.itil.org/en/ vomkennen/itil/ueberblick/index.php_itilv3_and_information_security_white_paper_may09.pdf.

Kanno, Y. (2008). *Information Security Measures Benchmark (ISM-Benchmark)*. Information-technology Promotion Agency (IPA).

Magalhaes, R. (2013). The Journey to ISO 27001 (Part 1). Retrieved September 19, 2018, from http://techgenix.com/journey-iso-27001-part1/.

Nieva, R., Hautala, L., & NG, A. (2018). Facebook breach put data of 50 million users at risk. USA: CBS Interactive Inc.

Pedersen, A., & Bjørn-Andersen, N. (2011). *Towards a framework for understanding adoption, implementation and institutionalization of ITIL*. Proceedings of IRIS 2011. ed. / Timo Leino. Turku: Turku Centre for Computer Science, (5), 601-639.

Peña, J., Vicente, E., & Ocaña, A. (2013). ITIL, COBIT and EFQM: Can They Work Together?. *International Journal of Combinatorial Optimization Problems and Informatics,* 4(1), 54-64.

Pentildéa, J. J. S., Vicente, E. F., & Ocantildéa, A. M. (2013). ITIL, COBIT and EFQM: Can They Work Together? *International Journal of Combinatorial Optimization Problems and Informatics*, 4(1), 54.

Sharma, N., & Dash, P. (2012). Effectiveness of ISO 27001, As an Information Security Management System: An Analytical Study of Financial Aspects. Far East Journal of Psychology and Business, 9(3), 42-55.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology*, 5(2), 2170-2176.

Sumtumthip, W., & Wongpinunwatana, N. (2017). Survey on the information system threats of listed companies in stock exchange of Thailand. *Journal of Information Systems in Business*, 3(3), 46-55.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, 11(5), 23-29.

ThaiCERT. (2017). Threat Statistic. Retrieved December 2, 2017, from https://www.thaicert.or.th/statistics /statistics-en.html.

Tofan, D. C. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*, 3(3), 128-135.