International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

http://ijpsat.ijsht-journals.org
Vol. 10 No. 1 August 2018, pp. 170-178

The Model of Quantifying Information Security With Cobit 5 Matrix in Indonesia Higher Education

IGN Mantra
Informatics Engineering
Perbanas Institute, Indonesia

Abstract **–Currently in the era of Industry 4.0, information security and cyber security becomes very important for all areas of government, private and education. The information produced by each party shall be maintained from the disturbance of various things, both natural disturbances and human disturbances. This paper examines more deeply about the quantification of information security with COBIT 5 Information Security approach and information security calculation matrix of each criterion especially in Higher Education only, since it has not been done by educational practitioners and all academicians to maintain and secure information resulting from. The outcome of this research is the degree of inventory criteria of information security function that is the current, expected and maximum degree. Object of in-depth research on campus Perbanas Insititut with degree "0" ie there is no Director of Information Security, Assessment of threats and vulnerabilities, Vulnerability management and incident response, including Business continuity and disaster recovery. For the distribution of questionnaires of respondents good results above 60% are Q1, Q2, Q5, Q7, Q11, Q13, Q23, Q25 and Q27, details can be seen in the study outcome table. Furthermore, this study produces an information security matrix for the 14 prescribed aspects of the COBIT 5 information security security risk. The information security posture will produce good information when the security matrix indicator is over 2 to 5, ie 2 (managed), 3 (established), 4 (predictable) and 5 (optimized). The average Higher Education in Indonesia is still in the COBIT 5 information security matrix below 2.**

Keywords **– Quantification, Information Security, COBIT 5 Matrix, Higher Education, Assesment, Vulnerability Management**

I. INTRODUCTION

Information Security Organizations such as protecting our Brain in the body, when our brain is sick and attacked by illness then paralyzed all the organs in our body, as well as the Organization Information, Information must be protected, should not be circulated to unauthorized parties. Lots of sensitive information must be protected and saved from evil hands, both external and internal.

Because sensitive information should be protected by all parties, whether staff up to the president director / senior organization, it is necessary to do some stages of information security protection. The author examines the quantification of information security by starting to measure the information security gap own company with the COBIT 5 Information Security approach, what is COBIT 5 Security ?, what should be quantified, how far the quantification find ?, what to do after getting the report about quantification in my own organization? will be discussed in more detail.

Information Security The organization is the organization's main asset and information resource. As we know there is a very important triangle in ICT namely People, Process and Technology, all three are very important and have an effect on the information security of the organization, because it plays a role for organizational progress in the distribution of information to public, economy, business, social, defense and security, law, culture and politics nationally.

COBIT 5 Information Security is a comprehensive frame work service to the triangle of interest that is to help government, private and education in information technology management to achieve organizational goals and goals in the future.

COBIT Focus 5 Information Security will provide a complete overview of both theory and practice as a guide for ICT leaders and staff for information security protection whether managing, managing both assets and ICT resources within the organization.

Corresponding Author: IGN Mantra

Main Objectives of COBIT 5 Information Security are:

1. Responsibility for ICT functions in the field of information security.
2. Improve the various aspects of leadership effectiveness and information security management within organizations, organizational rules and cultures.
3. Improve the relationship and information security network for organizational goals and objectives.
4. Maintain risk, integrity and protect information security at managerial and staff levels so that information is not misused.
5. Ensuring that ICT services and systems can be used sustainably both internally and externally.
6. Follow good governance laws and regulations that apply within the organization.
7. As a guide, an important aspect in the use of operational information security for the organization.

II. THE PROBLEMS

The COBIT quantification model 5 Information Security is a process of identifying and classifying the existence of an information security risk held within an organization.

For research that will be done this can summarized a number of problem formulation as follows:

1. The absence of quantified information security model in organizations, especially Higher Education in Indonesia.
2. The absence of quantification calculations of information security risks within the organization.
3. The absence of the COBIT 5 Security matrix to better describe the risk of information security within the organization.
4. The absence of specific / specific guidelines for the preparation of COBIT 5 Information Security effectively on information security governance in higher education organizations.

III. RESEARCH PURPOSES

1. The existence of the Information Quantification Quantification Model within the organization.
2. The quantification of information security risks within the organization is calculated.
3. The existence of a matrix with COBIT 5 Security to better describe the risk of information security within the organization.
4. The existence of specific / specific guidelines for the preparation of COBIT 5 Security or Information Security effectively on information security governance in organizations, especially Higher Education in Indonesia.

IV. RESEARCH METHODOLOGY

The methodology used for this research is a constructive research method to create an Information Security quantification model with the COBIT 5 Security Matrix. This model uses several tools used in quantifying information security.

Cobit 5 Security Matrix will perform a complete quantification both theory and practical to know and do information security protection both management, asset management and ICT resources within the organization.

Further analysis, testing of hazard errors in the design of publicly accessible information, will get deeper and more important information such as information security used.

Further above issues are solved by conducting literature studies, field studies and analysis of results obtained from direct testing of information security that has the potential to be applied for quantification. There are steps taken on the part of the applied methodology to get good results from the quantification model.

V. ANALYSIS AND DISCUSSION

Description of Research Objects

The study uses the Information Security Framework based on COBIT 5 Information Security to determine the effectiveness of the implementation of information security within educational organizations (universities) to prevent and reduce the risk of cyber attack on higher education / university processes, especially in Indonesia.

The research approach uses qualitative and quantitative in order to determine perceptions and views on sensitive issues related to various things in COBIT 5 IS Security such as:

1. Policies, principles and frameworks
2. Process
3. Organizational Structure
4. Culture, Ethics and Environment
5. Type Information
6. Service Ability
7. HR, Expertise and Competence

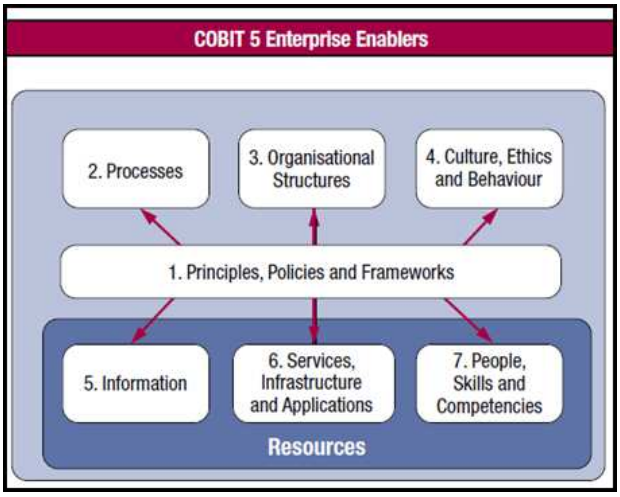

Fig.1,. Cobit 5 Security, Enterprise Enabler

The basis of this research is to determine how effectively the implementation of the Information Security System Framework COBIT 5 (IS) for Information Security in preventing and reducing the risk of cyber attacks on SCMS. This research combines qualitative and quantitative approaches to better in the context of information security so as to determine perceptions and views on issues relating to Network System Integrity, Intrusion Detection and Monitoring including Physical Security.

Moreover, issues concerning Information Systems Management for various tools from Third Party, Application Architecture Relations & Integration will be examined at the Information Systems Management Bureau. This study will also examine the reliability of the Security Framework Management System (COBIT 5 IS Security), Data Audit Line and Process Documentation.

According to Gratton & Jones, (2004), Experts use their own deductive and inductive strategies to apply and develop research goals and objectives. Scholars navigate through triangulation methods using a variety of study methods, emphasizing the use of various design philosophies and approaches to help improve the depth of understanding that can result from surveying.

According to (Hussey & Hussey 1997), Thus, this study follows a technique that includes a questionnaire survey and its supporters. The accuracy of qualitative and quantitative techniques is based on the questions surveyed or the questions asked. A researcher will use both methods as it offers extensive experience and a comprehensive understanding of the aims of a research confirming on the preference between quantitative and qualitative techniques in field studies. Different scholars have sought to distinguish between quantitative and qualitative methods of study: quantitative study techniques that originally evolved in the natural sciences for research on natural occurrences. Examples of triangulation methods are well established now in the social sciences. They are survey techniques, formal techniques (eg econometrics) arithmetic methods such as mathematical modeling and experimentation.

To be able to implement COBIT 5 Information Security should be done governance in Information Security at the University in general with various stages:

1. Meeting with Stakeholders to see needs.
2. Reviewing the Organization from the beginning to the end of the process.
3. Apply 1 Integrated Framework.
4. Doing a holistic approach
5. Separating Management with Management.

The following is the Key of Area Management and Management at the university by applying COBIT 5 Information Security,

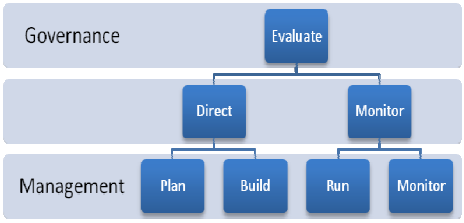

Fig.2,. COBIT 5 Security Governance and Management Criteria for measuring and degree of Compliamence to 5.1 COBIT 5 Information Security.

Information Security must have inventory capabilities and functions for components in the implementation of the Information Security Risk Management strategy. These functions will include elements such as threat and vulnerability assessment, vulnerability management, business resilience, architecture and design, and more. The KPIs established for information security will measure the organization's ability to maintain the risk tolerance level established by the risk management function.

Table 1,. Measurement and degree of Compliamence to 5.1 COBIT 5 Information Security.

Unit	Section	Evalution Criteria **0 : Incomplete** **1 : Performed** **2 : Managed** **3 : Established** **4 : Predictable** **5 : Optimized**	Current Level	Desired Level
5	Security Policy			
5.1	Information Security Policy	0. There is no documented security policy 1. The security policy applies to certain departments or units in the organization. 2. Security policy is documented and addresses all areas. 3. Security policy defines the responsibilities and sets the framework for all lines of business. The documentation is compiled. 4. Security policy and the associated documentation are reviewed regularly. The policy is adapted for the needs of all business lines. 5. Each employee knows the security policy. The organization regularly adapts the policy, the directives and associated documentation .	2	3

Table 2. Testing Resu Criteria for measuring and degree of compliamence

Unit	Section	Evaluation Criteria **0 : Incomplete** **1 : Performed** **2 : Managed** **3 : Established** **4 : Predictable** **5 : Optimized**	Current Level	Desired Level
1	CISO		1	3
2	Threat and Vulnerability Assesment		1	3
3	Vulnerability Management and Incident Response		1	3
4	Legal and Regulatory		3	4
5	Strategy		3	4
6	Policies, procedures, principles and standards		3	4
7	Business Continuance and disaster recovery		1	3
8	Education and communication		3	4
9	Program Governance		3	4
10	Architecture and design		3	4
11	Technology and capability evaluation		3	4
12	Key performance analysis and effectiveness		3	4
13	Information security Oversight board		1	3
14	Fraud		3	4

Information Security Functional Inventory

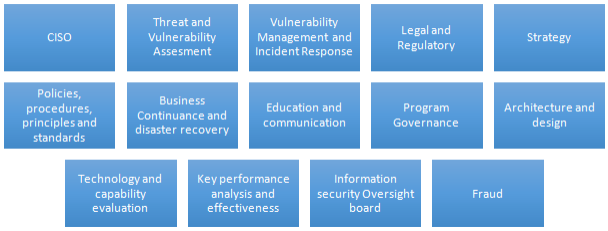

Fig.3,. Functional Inventory with COBIT 5 Information Security

While to know the degree of each Inventory Criteria of Information Security Function of Higher Education of Indonesia, can be seen table .1 and table .2, following,

A. Research Results with Table Degree and Chart

Result of research with result of processed table degree and chart as following,

Table 3. Degree of Inventory Criteria Information Security Function in Higher Education Indonesia (sample, Perbanas Institute, Jakarta), Information Security Matrix using COBIT 5.

Unit	Section	Evaluation Criteria 0 : Incomplete 1 : Performed 2 : Managed 3 : Established 4 : Predictable 5 : Optimized	Current Level	Desired Level
1	CISO	0	1	3
2	Threat and Vulnerability Assesment	0	1	3
3	Vulnerability Management and Incident Response	0	1	3
4	Legal and Regulatory	2	3	4
5	Strategy	2	3	4
6	Policies, procedures, principles and standards	2	3	4
7	Business Continuance and disaster recovery	0	1	3
8	Education and communication	2	3	4
9	Program Governance	2	3	4
10	Architecture and design	2	3	4
11	Technology and capability evaluation	2	3	4
12	Key performance analysis and effectiveness	2	3	4
13	Information security Oversight board	0	1	3
14	Fraud	2	3	4

The results of the calculation of the Maturity Information Security Model at Perbanas Institute are as follows,

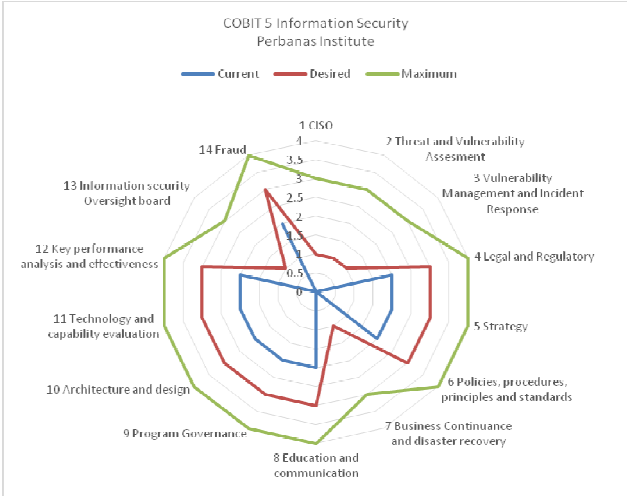

Fig.4,. Inventory Criteria Information Security Function at Perbanas Institute

B. Research Results with Questionnaire

This questionnaire was distributed to 33 users / respondents of Higher Education in Indonesia especially DKI Jakarta and Bandung only, Results / Finding from this questionnaire obtained:

Table 4. Results Questionnaire from 33 users / respondent of Higher Education in Indonesia, DKI Jakarta for Inventory criterion of Information Security Organization Function.

Unit	Criteria	Results Answers : Yes
1	Chief of Information Security Officer (CISO) Q1. Is there an Information Security Director (CISO) already? Q2. Is there a driver for Information Security Governance?	64% 45%
2	Threats and Vulnerability Assessment Q3. Have there been assessments of threats and vulnerabilities within the institution? Q4. Does the assessment of threats and vulnerabilities be done at least once a year?	70% 55%
3	Vulnerability Management and Incident Response Q5. Is there a management vulnerability already? Q6. Is there a vulnerability management team and an incident response?	88% 21%
4	Legal and Regulatory Q7. Are there any governance laws and regulations in the information security of institutions? Q8. Are there law enforcement and regulation in institutional information security?	88% 55%
5	Strategy Q9. Are there any strategies in information security governance? Q10. Has the strategy been used for every information governance implementation?	48% 12%
6	Policies, procedures, principles and standards Q11. Are there policies, procedures and standards in information security governance? Q12. Do you care about policies, procedures and standards in information security governance?	79% 52%

Unit	Criteria	Results Answers : Yes
7	Business Continuity and Disaster Recovery Q13. Is there a business continuity planning and disaster recovery in information security governance? Q14. Have you ever implemented business continuity and disaster recovery?	85% 24%
8	Education and Communication Q15. Are there education and communication in information security governance? Q16. Is the implementation of education and communication carried out continuously?	85% 39%
9	Program Governance Q17. Is there an information security governance program already? Q18. Is the governance program done every year?	33% 21%
10	Architecture and Design Q19. Are there architectures and designs for information security governance? Q20. Is the architecture and design of information security governance performed every time / year?	39% 27%
11	Technology and Capabilities Evaluation Q21. Has there been a technology evaluation and information security governance capability? Q22. Are technology evaluations and capabilities performed every time?	55% 30%
12	Key Performance Analysis and Effectiveness Q23. Is there a major performance analysis and effectiveness in information security governance? Q24. What is the utmost performance analysis and effectiveness performed every time?	85% 42%
13	Information Security Oversight Board Q25. Is there an information security	85% 18%

	supervisory board? Q26. Does it use information security supervisory boards every time?	
14	Fraud Q27. Are there any cases of information security fraud within the institution? Q28. Does information security fraud occur frequently?	61% 3%

From the table above the authors summarize the results for the criteria of the question with the biggest answer only more than (> = 60%) answered "Yes" is as follows:

Findings / Findings

Q1. Is there a Director of Information Security (CISO)? The answer of respondents is 64%. It can be argued that most institutions in Higher Education do not have the position of Director of Information Security or CISO, even if there are still very limited information security functions.

Q3. Are there any threat and vulnerability assessments within the institution ?, The respondents' answers are 70%. It can be argued that in Higher Education there has been a threat and vulnerability assessment and this is a good opportunity to improve this security assessment every 1 year.

Q5. Are there any vulnerability management ?, Responders' answers are 88%, very good because there is already vulnerability management in every higher education to be upgraded to the vulnerability management team and response incident.

Q11. Are there policies, procedures and standards in information governance? The respondents' answers are 79%, there are good policies, procedures and standards in information security governance in each Higher Education.

Q13. Are there any business continuity plans and disaster recovery in information security governance ?, The respondents' answers are 85%, very good, they are in Higher Education already concerned about business continuity plans in case of disaster, fear and concerns of users for their data and information safe despite the disaster.

Q15. Are there already education and communication in information security governance? Responders' answers are 85%, very good, Higher Education Institutions have good education and communication in information security governance in each campus, there is a concern to learn and communicate about this matter.

Q23. Is there a major performance analysis and effectiveness in information security governance ?, Responders' answers are 85%, it is good that in Higher Education there is a major performance analysis and effectiveness in information security governance so that in the future it will be further enhanced in the analysis.

Q25. Is there an information security supervisor ?, The correspondent's answer is 85%, very good, since the users in Higher Education already have a surveillance board for information security itself, the presence of intruders etc. can be quickly identified.

Q27. Is there an information security fraud case in the institution ?, The correspondent's answer is 61%, meaning there are some cases of information security fraud in each institution, to the extent that the depth of the case still needs to be studied further.

VI. CONCLUSIONS

This study was conducted within 6 months since beginning of January 2018, the basic tools used are COBIT 5 Information Security, as the world standard is undoubtedly to determine the level of maturity level of the organization in conducting information security governance in each of its organizations .

The authors chose the object of research in the area of campus or Higher Education in Indonesia, the number of campuses in Indonesia is quite large, more than 3000 campuses are active, and 3000 the following is still not clear to the actives. The author sees there is still no comprehensive information security governance, from the above research data can be retrieved.

A. Conclusion

1. Good information security governance framework and implementation has not been well used in all campuses in Indonesia.
2. There are several campuses that have begun to think about information security but have not used the rules of governance and information security framework well and detail (depth).
3. The maturity level of information security governance with COBIT 5 tools is still below 2, meaning that it has not used good information security governance (bad).
4. The results of the questionnaire have obtained a good overview or portrait of information security governance postures and the frameworks of only a few correspondents well and clearly provide information that information security governance has not been used in higher education institutions in Indonesia.
5. Average Answers The questionnaires of respondents below 60% responded to the condition / status of the campus information security portfolio, in other words still poor and not yet implemented information security governance within the campus of Indonesia.

B. Recommendation

1. Conducting further research on information security risk management in Higher Education Indonesia.
2. Measure the next Balanced Score Card Metrics Security in Higher Education Indonesia.
3. Recalculate the degree of information security in Higher Education Indonesia then conduct compliance with the standards to be selected such as COBIT 5 Information Security, ISO 27001 or NIST.
4. Create a composite standard for Information Security in Higher Education Indonesia with triangle COBIT 5 Information Security, ISO 27001 and NIST.

Thus the results of this research may be used well for information security governance elsewhere.

REFERENCE

[1] Andrei Ioan Hohan, Marieta Olaru, Ionela Carmen Pirnea. (2015), Assessment and continuous improvement of information security based on TQM and business excellence principles, Emerging Markets Queries in Finance and Business, Procedia Economics and Finance 32 (2015) 352 – 359

[2] Braeuer J., Ploesch R., Saft M. (2017) Measuring Maintainability of OO-Software - Validating the IT-CISQ Quality Model. In: Janech J., Kostolny J., Gratkowski T. (eds) Proceedings of the 2015 Federated Conference on Software Development and Object Technologies. SDOT 2015. Advances in Intelligent Systems and Computing, vol 511. Springer, Cham

[3] Ciptaningrum, D., Nugroho, E., & Adhipta, D. (2015). Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5. Sentika, 2015(Sentika), Seminar Nasional Teknologi Informasi dan Komunikasi 2015 (SENTIKA 2015), ISSN: 2089-9815, pp. 65-74.

[4] Fitrianah, D., & Sucahyo, Y. G. (2013). Audit Sistem Informasi/Teknologi Informasi dengan Kerangka Kerja COBIT untuk Evaluasi Manajemen Teknologi Informasi di Universitas XYZ. *Journal of Chemical Information and Modeling*, 53(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

[5] Hanim Maria Astuti, Feby Artwodini Muqtadiroh, Eko Wahyu Tyas Darmaningrat, Chitra Utami Putri. (2017), Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk, 4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia, Procedia Computer Science 124 (2017) 569–576.

[6] I. G. So et al., "Action Design of Information Systems Security Governance for Bank Using COBIT 4.1 and Control Standard of ISO 27001", Advanced Materials Research, Vol. 905, pp. 663-668, 2014

[7] Knut Haufe, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis,Vladimir Stantchev. (2016). ISMS core processes: A study, Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016, Procedia Computer Science 100 (2016) 339 – 346

[8] Knut Haufe, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis,Vladimir Stantchev. (2016), Security Management Standards: A Mapping, Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016, Procedia Computer Science 100 (2016) 755 – 761.