ASSESSEMENT WEB SECURITY AND DATA SECURITY ON PRIVATE CLOUD COMPUTING

DEVENDHAR NAYINI
Assistant professor, Dept. of Information Technology, Mahaveer Institute of Science & Technology, Bandlaguda, Hyd, India,
devendharnayini1224@gmail.com

K.PRIYANKA
Assistant professor, Dept. of Information Technology, Mahaveer Institute of Science & Technology, Bandlaguda, Hyd, India,
priyankakamatham@outlook.com

ABSTRACT

Data security is an essential topic that contributes the success of business operation nowadays. The high need of applying efficacious Data Security is visualized seen in all business and non-profit entities. The artefact takes the instance of university XYZ that uses Private Cloud Computing as essential tools to support its business processes. The artefact explores the effective way of measuring the level of Data Security and Web Security performance highlights more on Private Cloud undergoing its recommendations. Web Security is used to measure the Data Security and Web Security performance, respectively. The thing identifies the maturity level space between present and expected results that provides required recommendation to improve present situation. The result of the artefact is expected to provide as credentials for Data security application in Higher Education Organizations.

Keywords: *Information Security, Cyber Security, Private Cloud Computing, ISO 27001, COBIT 5.*

1 INTRODUCTION

Cloud Computing in the function of information technology requires standards and procedures[1], especially Private Cloud Computing where the Information Technology is managed thoroughly by the organization itself, both from the provision of infrastructure to the allocation of resources in agreement with the capacity of users[2].

Cloud computing was being distributed in all sectors of works throughout, especially in Educational institutions[3]. Based on analysis by ViON and Hitachi[4], it is known that Higher Education Institutions are using the cloud to manage a wide range of technology, administrative, and educational systems, from nuts-and bolts services to more contemporary applications. This analysis also identifies that the pre-dominant model of the cloud computing in higher education is a private cloud model capitalized by operating expenses.

Novelty of the new technology inherting will increase the threat involved, if not managed well[5,6]. Recent cyber attacks prove that Educational Institutions are one of the major target of the hackers[7]. Based on this analysis, it is identified that in 2014, 10 percent of security is violated, involved the education sector. Based on another artefact[8], it is well-known that globally pre-dominant universities such as Harvard, is attacked by unknown hacker.

University XYZ is an Educational Institution that uses Private Cloud Computing as one of the major pedestal of Information Technology in reinforcing organizational business processes. Based from the record of firewall in the University XYZ, presently there's about 1 million obstrusions detected over year targeted on its Private Cloud Computing. Given this Private Cloud Computing is one of the crucial IT Information Security needed in improving customer satisfaction, where staff and students are considered here.

Therefore, it is essential to measure the level of Information Security maturity focused on Private Cloud Computing owned by University XYZ. At University XYZ, no information security measures have been taken so that measurements are needed to determine the conditions of information security implementation at University XYZ.

Maturity model can increase the potentiality and efficiency of security programs by focusing on thorough and repeatable security process that can self improve and integrated into the overall operational infrastructure[9].

Assessment and evaluation of investments that have been issued for IT implementation also has to be well considered. Based on the research done before, explained that the organization has begun to realize and start doing performance measurement and evaluation[10,11]. In analyzing IT, there are several frameworks that serve as international guidelines in IT governance which has been implemented widely and has proven its implementation such as ISO 27001[12], COBIT[13,14], ITIL[15].

Information security plays an vital role and becomes an prominent issue in assessing system effectiveness[16,17]. ISO 27001:2013 is an international standard that identifies the need to provide, manage, and improve information security management systems[18] and used as a credentials in the measurement and control of information security[11].

Another framework for securing the information technology and Cyber Security is COBIT 5. COBIT 5 for Cyber Security encompasses all of the general Information Technology controls, which is dedicated for achieving overall information technology security[19].

This research provides mapping from COBIT 5 for Cyber Security section *Applying Cyber Security* processes to ISO27001:2013 as well as the majority level analysis for both in University XYZ.

2 THEORETICAL FRAMEWORK AND LITERATURE ASSESSMENT

Information Security refers to the term that enables to protect the computer system from illegal, to provide Confidentiality, Integrity and Availability[20].

Information Security has several important aspects that are known as C.I.A Triad [21], which consists of aspects of Confidentiality, Integrity, and Availability[22].

Confidentiality(C) ensures that sensitive information are accessed only by an authorized person and kept away from those are not authorised to possess them.

Integrity (I) ensures that information are in a format that is true and correct to this original purposes. The receiver of the information must have the information, the creator intended him to have. Availability (A) ensure that information and Cloud Computing is a distributed computing paradigm that was focused on providing a wide range of users that makes use of existing technologies such as virtualization, service- orientation, and grid computing, to acquire and manage IT resources on a large scale[2]. Cloud computing's paradigm encompasses access to a shared pool of computing resources that can be rapidly provisioned and released with minimal effort[23]. NIST defines Cloud Computing definition[23], comprised of five essential characteristics, three service models, and four deployment models. Four deployment models on cloud computing[24] can be summarized as: (1) Private cloud(2) Community cloud, (3) Public cloud (4) Hybrid cloud

Security in Cloud Computing

Security and the privacy issues in cloud computing has received extensive attentions recently[29]. Scholars summarized the cloud into two categories: (1) cloud storage security, and (2) cloud computation security. Both studies shows important eight different aspects[30], such as (1) Privacy and trust; (2) Internet and Services; (3) Access; (4) Storage and Computing; (5) Software; (6) Virtualization; (7) Network; and (8) Compliance & Legality. Various framework and recommendation has been created to evaluate maturity index and mitigate the risk that emerge from these aspects[26,29,31– 34]. Most of the research use only information security framework, e.g. ISO 27k series[26,29,31,32] or Cyber Security framework, e.g. NIST Cyber Security Framework[33,34]. This research tried to evaluate and incorporate the popular information security framework ISO27k series with the emerging Cyber Security and IT Governance framework, the

COBIT 5 for Cyber Security.

ISO 27001:2013 for Cloud Computing

Tariq [35] states that information security responsibilities' that are delegated to vendors and organizations differ depending on the cloud computing scenario used by an organization. The scenario consists of 4 types: in-house or private, *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS), and *Software-as-a- Service* (SaaS). Details of organizational and vendor responsibilities on cloud computing with each scenario can be seen in

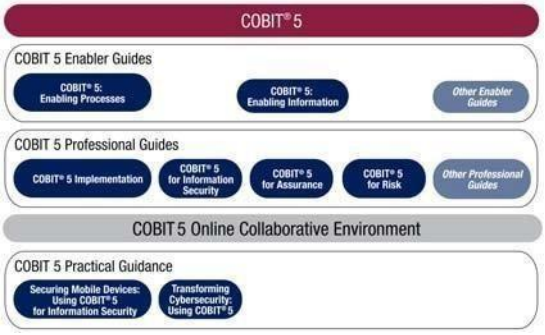

Figure 2 COBIT 5 Product Family, adopted from [19]

Professional Guides for COBIT 5 – *COBIT 5 for Information Security* in Figure 2, have 2 additional practical guidance which can be fit and aligned with the ISO27001:2013, *Securing Mobile Devices Using COBIT 5 for Information Security* and *Transforming Cyber security Using COBIT 5.* In this paper, author focused on the latter, based on COBIT 5 for Cyber Security[19].

COBIT 5 for Cyber Security

Cyber security encompasses all that protect enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences[19,36]. COBIT 5 not only can be used for IT Governance, but can be used as a controller for Information Security and Cyber security. COBIT 5 for Cyber security divided into several processes: (1) Cyber security Governance; (2) Cyber security Business Case; (3) Applying to Cyber security; (4) Cyber security Management; and (5) Cyber security Monitoring. This paper use the third process, Applying to Cyber security Process, which description can be seen in Table 1.

Table 1 COBIT 5 Applying to Cyber security Processes, adopted from [19]

Process	Description
APO13	**Manage security**
APO13.01	Establish and maintain an information security management system (ISMS)
APO13.02	Define and manage and information security risk treatment plan
APO13.03	Monitor and review the ISMS
DSS05	**Manage security services**
DSS05.01	Protect against malware
DSS05.02	Manage network and connectivity security
DSS05.03	Manage endpoint security
DSS05.04	Manage user identity and logical access

Maturity Level Framework

SSE-CMM

Systems Security Engineering - Capability Maturity Model, or SSE-CMM, is a model developed for the purpose of advancing security techniques as defined, mature and scalable disciplines [37]. In its development, this SSE-CMM entered into ISO 21827:2008[38]. This CMM approach is done to (1) define accepted ways to improve process capability; (2) increase usage in acquisitions as an indicator of process capability.

In SSE-CMM, there are 6 levels of ability that indicate the level of maturity of a process that can be seen in Table 2.

Table 2 Capability Level in SSE-CMM

Level	Definition
Level 0	not all base practices are performed
Level 1	all the base practices are performed but informally, meaning that there is no documentation, no standards and is done separately

Level 2	plan & track, which indicates commitment planning process standards
Level 3	well defined meaning standard process has been run in accordance with the definition
Level 4	controlled quantitatively, which means improved quality through monitoring of every process
Level 5	improved constantly indicating the standard has been perfect and the focus to adapt to changes.

In the SSE-CMM method, scoring assessments in each process area are selected from 0 to 5 for each process area [11].

Maturity Level

A mature information system has the ability to manage good development and management[39]. Maturity of an information system could be measured using a tool called Maturity Level.

This maturity level model is based on software evaluation methods so that the organization can self-evaluate from level 0 (none) to level 5 (optimal).

This maturity model is developed with the aim of continuous process improvement. Each level of maturity consists of a set of process objectives that, if met, will stabilize an important component of the on the findings in the questionnaire. This data analysis includes Measuring the performance of the information security maturity level on cloud computing in University XYZ IT departments and Gap Analysis from the expected maturity level with field realities.

Mapping ISO27001:2013 to COBIT 5 for Cyber Security

The basic difference between COBIT 5 for Cyber Security and ISO27001:2013 was that ISO27001:2013 focused only on information security and COBIT 5 for Cyber Security is focused on IT Governance with additional control for Cyber Security. Thus, COBIT 5 for Cyber Security covers a broader range of general information technology topics, but was not having information security requirements as detailed as described in ISO27001:2013.

Previous research by Rosmiati[11] only covers the information security and this research further extends the research to incorporate the Cyber Security by using COBIT 5 for Cyber Security in a new mapping model.

In order to coordinating and complementing both ISO27001:2013 and COBIT 5 for Cyber Security, a mapping between both is beneficial. The purpose of the mapping is providing an integrated way for applying Cyber Security in COBIT 5 for Cyber Security and achieving the ISO27001:2013 information security management. Mapping of these process enables the organization to apply both Cyber Security and Information Security, thus effectively manage risks and reduce the overall risk levels.

For the mapping of these frameworks, every COBIT 5 for Cyber Security section Applying to Cyber Security process is investigated, and the corresponding ISO27001:2013 Annex A control objectives are indicated. Based on this research, the mapping of ISO27001:2013 control objectives and COBIT 5 for Cyber Security processes can be seen in Table 6.

Table 6 Mapping of COBIT 5 for Cyber Security to ISO27001:2013

COBIT 5 Cyber Security (Applying to Cyber Security) Process		**ISO27001:2013 Control Objectives**	
APO13	**Manage security**		
APO13.01	Establish and maintain an information security management system (ISMS)	A.5.1	Management direction for information security
		A.6.1	Internal organization

APO13.02	Define and manage and information security risk treatment plan	A.12.3	Backup
		A.16.1	Management of information security incidents and improvement
		A.17.2	Redundancies
APO13.03	Monitor and review the ISMS	A.17.1	Information security continuity
		A.18.1	Compliance with legal and contractual requirements
DSS05	**Manage security services**		
DSS05.01	Protect against malware	A.12.2	Protection from malware
DSS05.02	Manage network and connectivity security	A.10.1	Cryptographic controls
		A.13.1	Network security management
		A.13.2	Information transfer
DSS05.03	Manage endpoint security	A.6.2	Mobile device and teleworking
		A.11.2	Equipment
DSS05.04	Manage user identity and logical access	A.9.2	User access management
		A.9.3	User responsibilities
		A.9.4	System and application access control
DSS05.05	Manage physical access to IT assets	A.11.1	Secure areas
DSS05.06	Manage sensitive documents and output	A.8.1	Responsibility for assets

Company Profile & Evaluation

University XYZ is one of the private universities in Indonesia. The university has been using private cloud computing installed on blade servers since 2010. In its development, the university wants better policy and information security controls in using private cloud computing. Based on this, XYZ University wants an evaluation of existing information security controls.

Organizational Structure

University XYZ is chaired by a rector and assisted by 4 vice rectors each with their respective sections. Vice Rector 1 is an expert in general administration and finance, Vice Rector 2 is an expert in academics, Vice Rector 3 is an expert in the field of student affairs, and Vice Rector 4 is an expert in the field of relations and cooperation. IT departments are directly under the vice rector 1.

Organizational Structure in IT Department

IT Department at XYZ University is chaired by an IT manager and consists of 4 parts: IT Support consisting of 4 persons, 4 programmers, Network engineer consisting of 2 people: 1 as network administrator and 1 as system administrator, and 1 person as a helpdesk. In the development, configuration settings, as well as monitoring on private cloud computing, network engineers have the most important role.

Evaluation on existing systems

The current system is highly dependent on private cloud computing owned by the university. Almost all of the deployed systems are on the cloud computing cloud blade servers of universities such as university main sites with all existing sub-systems, such as student applications, university internal applications, library applications, etc.

Based on the observations on the installed firewall, it is known that the attack statistical classification in april 2017 s.d. april 2018 can be seen in Figure 4.

Based on this observation, top 3

intrusion event was: (1) Network trojan, with 504.641 events; (2) Misc activity, with 348.162 events; and (3) Potential corporate policy violation, with 100.318 events.

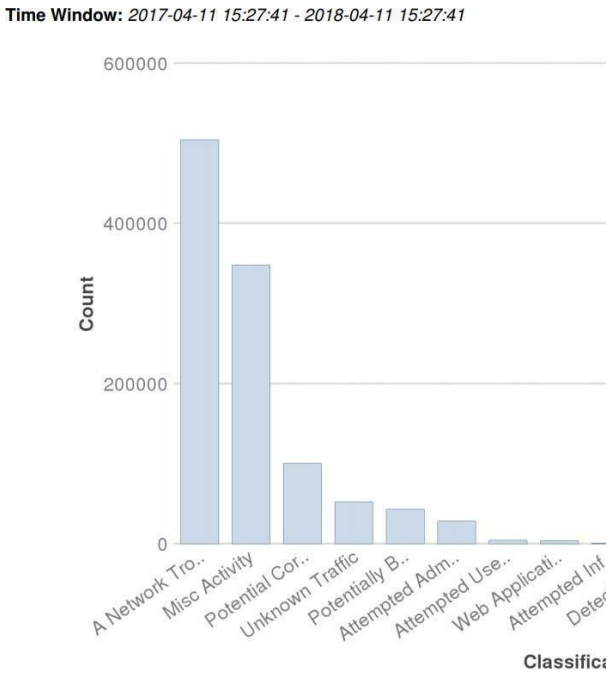

Figure 4 Intrusion event and its classification

3 FINDINGS AND STRATEGY FOR INFROMATION SECURITY

Maturity Level University XYZ

Based on the processed questionnaire of University XYZ's IT department, the maturity level of University XYZ's private cloud computing information security is shown in Table 7.

Table 7 Maturity level of Information Security in Private Cloud Computing of University XYZ

Annex No (Clauses)	Score	Maturity Level
A.5	2.75	3 – Established
A.6	2.34	2 – Managed
A.7	2.76	3 – Established
A.8	2.66	3 – Established
A.9	2.84	3 – Established
A.10	1.41	1 – Performed
A.11	2.66	3 – Established
A.12	2.38	2 – Managed
A.13	2.27	2 – Managed
A.14	2.39	2 – Managed
A.15	1.89	2 – Managed
A.16	1.98	2 – Managed
A.17	2.09	2 – Managed
A.18	1.94	2 – Managed
AVERAGE	2.31	2 – Managed

The result of processed questionnaire data shows Based on this result and the mapping reference from COBIT5 for Cyber Security process to ISO27001:2013, Maturity level for COBIT5 for Cyber Security process can be seen in Table 8.

Table 8 Maturity level of Cyber Security in Private Cloud Computing of University XYZ

Process	Score	Maturity Level
APO13.01	2.75	3 - Established
APO13.02	2.28	2 - Managed
APO13.03	2.14	2 - Managed
DSS05.01	3.00	3 - Established
DSS05.02	1.99	2 - Managed
DSS05.03	2.27	2 - Managed
DSS05.04	2.74	3 - Established
DSS05.05	2.69	3 - Established
DSS05.06	2.66	3 - Established
DSS05.07	1.91	2 - Managed
AVERAGE	2.44	2 - Managed

The result of the mapping process shows that the average value of Cyber Security appliance of private cloud computing at University XYZ is 2.44. This value indicates that the Cyber Security of

private cloud computing exists at the second level too, i.e. Managed. Based on the results in the Table 8, for each COBIT5 for Cyber Security process, a graph of maturity level can be seen in Figure 6. that the average value of information security control of private cloud computing at University XYZ is 2.31. This value indicates that the security of private cloud computing information exists at the second level, i.e. Managed. Based on the results in Table 7, for each ISO 27001:2013 clause, a graph of maturity level can be seen in Figure 5.

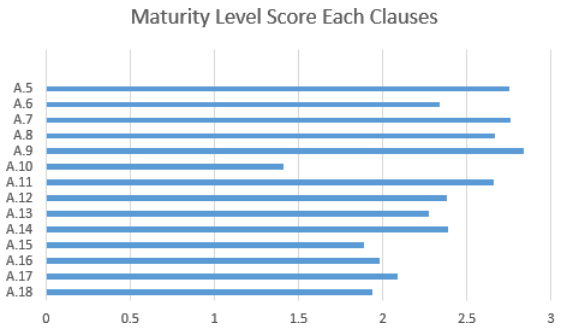

Figure 5 Graph of Maturity Level Score for Each Clause

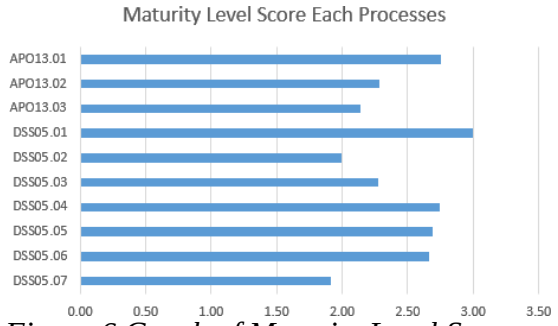

Figure 6 Graph of Maturity Level Score for Each Process

Gap Analysis

After knowing that the maturity level of private cloud computing information security is at 2.31 (Managed) and the maturity level of private cloud computing Cyber Security is at 2.44 (Managed), and the expected value of maturity level for both is 5 (Optimized). This expectation value of 5 is seen from the duration of private cloud computing usage of University XYZ (> 5 years) and the expectations of the University's stakeholder and the IT Manager who want good information security and Cyber Security readiness. Gap analysis to the maturity level can be seen in Table 9 and Table 10.

Table 9 Maturity Level Information Security Gap Analysis

Annex No (Clauses)	Current Score	xpected Score	Gap
A.5	2.75	5.00	2.25
A.6	2.34	5.00	2.66
A.7	2.76	5.00	2.24
A.8	2.66	5.00	2.34
A.9	2.84	5.00	2.16
A.10	1.41	5.00	3.59
A.11	2.66	5.00	2.34
A.12	2.38	5.00	2.62
A.13	2.27	5.00	2.73
A.14	2.39	5.00	2.61
A.15	1.89	5.00	3.11
A.16	1.98	5.00	3.02
A.17	2.09	5.00	2.91
A.18	1.94	5.00	3.06
AVERAGE			2.69

(Annex A.5), 2.66 (Annex A.6), 2.24 (Annex A.7),
2.34 (Annex A.8), 2.16 (Annex A.9), 3.59 (Annex A.10), 2.34 (Annex A.11), 2.11 (Annex A.12), 2.62 (Annex A.13), 2.61 (Annex A.14), 3.11 (Annex A.15), 3.02 (Annex A.16), 2.91 (Annex A.17), and 3.06 (Annex A.18).

From Table 10, it is known that the gap distance of Cyber Security appliance from the present condition to the expected condition for each process is 2.25 (APO13.01), 2.72 (APO13.02), 2.86 (APO13.03), 2.00 (DSS05.01), 3.01 (DSS05.02),
2.73 (DSS05.03), 2.26 (DSS05.04), 2.31
(DSS05.05), 2.34 (DSS05.06), and 3.09 (DSS05.07).

After knowing the gap distance from each clause and process, all of these values will be added and averaged to calculate the overall value of the gap.

The overall value of the information

security gap is known to be 2.69 between the current maturity level and expected maturity level and the overall value of the Cyber Security gap is known to be 2.56 between current maturity level and expected level.

Both of these values are quite large from the expected level of maturity that is required so that the necessary readjustment on any ISO controls and COBIT5 for Cyber Security processes that exist.

It is necessary to look for minimal / weak ISO control and COBIT5 for Cyber Security process by finding the ratio of the value of the current maturity level to the expected maturity level. These value ratios can be seen in Figure 7 and Figure 8.

Table 10 Maturity Level Cyber Security Gap Analysis

Process	Current Score	xpected Score	Gap
APO13.01	2.75	5.00	2.25
APO13.02	2.28	5.00	2.72
APO13.03	2.14	5.00	2.86
DSS05.01	3.00	5.00	2.00
DSS05.02	1.99	5.00	3.01
DSS05.03	2.27	5.00	2.73
DSS05.04	2.74	5.00	2.26
DSS05.05	2.69	5.00	2.31
DSS05.06	2.66	5.00	2.34
DSS05.07	1.91	5.00	3.09
AVERAGE			2.56

From Table 9 it is known that the gap distance of information security from the present condition to the expected condition for each clause is 2.25

Figure 7 Ratio Value Between Current Maturity Level and Expectations (ISO27001:2013)

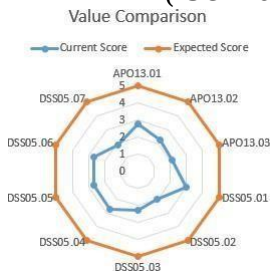

Figure 8 Ratio Value Between Current Maturity Level and Expectations (COBIT5 for Cyber Security)

Found several problems based on the highest gap level:

1. No policy on cryptography control has been implemented
2. The non-implementation of policies that govern the entire cryptography key cycle
3. Not yet applied risk management to supplier relationship
4. There has been no control over the limits of access to information and infrastructure between suppliers and University XYZ
5. No audit and evaluation of suppliers
6. Lack of legal identification and documentation
7. There is no policy of the organization that regulates the observation and use of paid tools, especially in the managerial device of cloud computing, has not been fully licensed
8. Lack of recording of loss and damage, as well as falsification of access to the use of cloud computing.
9. Absence of arrangements on compliance evaluation with applicable legal policies and procedures and compliance.

From the findings on this issue, a recommendation was made to improve the conditions of information security within

University XYZ. Among others are:

1. Enforce policies on the use of good cryptography, use SSL in the HTTP protocol and enforce a secure password policy.
2. Schedule updates to key cryptography (scheduled renewal)
3. Conduct risk management evaluation before using the goods from the supplier
4. Enforce control limitation from supplier, make policy about supplier's authorization to organization
5. Conducting periodic audits and evaluations of suppliers, may be an evaluation of conformity to SLAs.
6. Identify and documentation related to legal.
7. Establish a policy on the use of paid devices, purchase of licensed goods specifically in the case of managerial cloud computing
8. Establish a policy on recording incidents and attacks on cloud computing
9. Make policy on evaluation of policies and procedures that are in accordance with the existing laws in the University XYZ State located.

The result of measuring the maturity level of information security of private cloud computing at University XYZ shows that University XYZ's readiness is at level 2 (Managed). The results of the ISO 27001:2013 maturity questionnaire earned average results for each clause of 2.31 and after mapped into the COBIT5 for Cyber Security, section Applying to Security, earned the average results for each process is 2.44.

The gap value of the private cloud computing information security and Cyber Security condition to the expected value is 2.69 and 2.56. Based on this, it can be drawn the existing information security and Cyber Security problems related to private cloud computing is around the implementation of cryptography policy, the lack of limits and audits of suppliers, and the lack of policies related to legal compliance, lack of infrastructure monitoring policy, lack of network and connectivity security management, and lack of monitoring of the ISMS itself.

Future Work

This preliminary information security audit on private cloud computing is still using ISO 27001:2013 and COBIT5 for Security, Applying Cyber Security section as the standard and maturity level using the SSE-CMM assessment index adapted to ISO 15504-6:2013 capability levels. Further research could use other maturity models to compare the effectiveness of maturity models or use other standards related to cloud computing, e.g. ISO 27017/8:2013 and bigger section from COBIT5 for Cyber Security to further integrate not only the ISMS, but also the IT Governance.

CONCLUSION

The article has analyzed the probability that cloud computing, especially private cloud computing, can be used for higher education institution. Although cloud computing is considered a new technology for the higher education institution, it cannot be separated from the fact that it is prone fromattack.

The article presents an overview of current trend of the use of information security framework for private cloud computing in higher education institution. The article incorporates the advantages of ISO 27001:2013 and COBIT 5 for
Cyber Security framework to analyze and assess the use of information security and identify the cyber security capability (maturity level) of the private cloud computing at University XYZ.

The mapping model of this article provides analysis benefits such as: firstly, it enables mapping the security model that can give a comprehensive analysis for both the use of information security and cyber security readiness for the private cloud computing; secondly, the use of maturity level and gap analysis can point out the weak section of both information security and cyber-security of the private cloud computing, proposes for further development.

REFERENCES:

[1] Al Morsy M, Grundy J, Müller I. An analysis of the cloud computing security problem.

17th Asia-Pacific Softw Eng Conf (APSEC 2010) Cloud Work Aust 2010:7. doi:arXiv:1609.01107.

[2] Lewis G. Basics About Cloud Computing. Softw Eng Inst 2010

[3] Pardeshi VH. Cloud Computing for Higher Education Institutes: Architecture, Strategy and Recommendations for Effective Adaptation.Procedia Econ Financ 2014;11:589–99. doi:10.1016/S2212-671(14)00224-X.

[4] ViON, Hitachi. Trends in Cloud Computing in Higher Education Colleges and universities 2016.

[5] Barham BL, Chavas JP, Fitz D, Salas VR, Schechter L. The roles of risk and ambiguity in technology adoption. J Econ Behav Organ 2014;97:204–18. doi:10.1016/j.jebo.2013.06.014.

[6] Foster AD, Rosenzweig MR. Microeconomics of Technology Adoption. AnnuRev Econom 2010;2:395–424. doi:10.1146/annurev.economics.102308.12 4433.

[7] Wagstaff K, Sottile CA. Cyberattack 101: Why Hackers Are Going After Universities. NBCNews 2015.

[8] Harris CE, Hammergen LR. Higher education's vulnerability to cyber attacks. Univ BusMag 2016.

[9] Acohido B. Improving Detection , Prevention and Response with Security Maturity Modeling. Sans Inst 2015.

[10] Surbakti H. Cobit 4.1: A Maturity Level Framework For Measurement of Information System Performance (Case Study: Academic Bureau at Universitas Respati Yogyakarta). Int J Eng Res Technol 2014;3:999–1004. doi:2278-0181.

[11] Rosmiati, Riadi I, Prayudi Y. A Maturity Level Framework for Measurement of Information Security Performance. Int JComputAppl2016;141:975–8887. doi:10.5120/ijca2016907930.

[12] ISO/IEC. ISO/IEC 27001:2013(E) Information technology — Security techniques — Information security management systems — Requirements. ISOOrg [Online] 2013:1–24. doi:10.1109/IEEESTD.2005.339589.

[13] Isaca. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Isaca; 2013.

[14] Isaca. COBIT 5: Implementation. 2012.

[15] [15]Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33:236–47. doi:10.1080/0144929X.2012.708787.

[16] Sohrabi Safa N, Von Solms R, Furnell S. Information security policy compliance model in organizations. Comput Secur 2016;56:1–13. doi:10.1016/j.cose.2015.10.006.

[17] ISO/IEC. ISO/IEC 27000:2016(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISOOrg [Online] 2016;4th Editio:42.

[19] ISACA. Transforming Cybersecurity using COBIT 5. 2013.

[20] NIST. Guide for conducting risk assessments (NIST SP 800-30 R1). NIST Spec Publ 2012:95. doi:10.6028/NIST.SP.800-30r1.

[21] Perrin C. The CIA triad. Dostopno Na Techrepublic Com/Blog/Security/the-Cia-Triad/488 2008.

[22] Coss, D. Samonas S. The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. J Inf Syst Secur 2014;10:21–45.

[23] Mell P, Grance T. NIST Special Publication 800-145 Definition of Cloud Computing. Nist Spec Publ 2011;145:7. doi:10.1136/emj.2010.096966.

[24] Badger L, Patt-corner R, Voas J. NIST Special Publication 800-146 Cloud Computing Synopsis and Recommendations. Nist Spec Publ 2012;800:81. doi:2012.