Journal of Theoretical and Applied Information Technology
15th January 2019. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MEASURING INFORMATION SECURITY AND CYBERSECURITY ON PRIVATE CLOUD COMPUTING

[1]WENDY, [2]WANG GUNAWAN

[1,2] Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia, 11480.

E-mail: [1]wendy.hardianto@binus.acid; [2]gwang@binus.edu;

ABSTRACT

Information security is an essential topic that contributes the success of business operation nowadays. The urgency of applying effective information security can be seen in all business and non-profit entities. The article takes the case of university XYZ that uses private cloud computing as essential tools to support its business processes. The article examines the effective way of measuring the level of information security and CyberSecurity performance that focuses on private cloud use with its recommendations. The article applies the ISO 27001:2013 framework by involving all clauses in Annex A ISO 27001:2013 and COBIT5 for CyberSecurity, section Applying to CyberSecurity. Annex A ISO 27001:2013 and COBIT5 for CyberSecurity is used to measure the information security and CyberSecurity performance, respectively. The article uses a survey method to the employees in the IT division at University XYZ. The article examines the maturity level gap between current and expected results and provides necessary recommendation to improve current situation. The outcome of the article is expected to provide as a reference for information security application in higher education institutions.

Keywords: *Information Security, CyberSecurity, 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 accordance with the capacity of users[2].

Cloud computing was being deployed in all sectors of works globally, especially in higher education[3]. Based on a research 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 innovative applications. This research also discover that the dominant model of the cloud computing in higher education is a private cloud model funded by operating expenses.

Novelty of the new technology adoption may increase the risk involved, if not controlled well[5,6]. Recent cyber attacks prove that higher education institution are one of the prime target of the hackers[7]. Based on this research, it is known that in 2014, 10 percent of reported security breach, involved the education sector. Based on another article[8], it is known that even the globally popular universities such as Harvard, is attacked by unknown hacker.

University XYZ is an educational institution that uses private cloud computing as one of the main pillars of information technology in supporting organizational business processes. Based from the log of firewall in the University XYZ, currently there's about 1 miliion intrusions detected per year targeted on its private cloud computing. Given this private cloud computing is one of the core IT information security needed in improving customer satisfaction, which in this case is the staff and students.

Therefore, it is necessary to assess 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 effectiveness 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].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Assessment and evaluation of investments that have been issued for IT implementation also need to be well considered. Based on the research that has been 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 that has been implemented widely and has proven its implementation such as ISO 27001[12], COBIT[13,14], ITIL[15].

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

Another framework for securing the information technology and CyberSecurity is COBIT 5. COBIT 5 for CyberSecurity 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 CyberSecurity section *Applying CyberSecurity* processes to ISO27001:2013 as well as the maturity level analysis for both in University XYZ.

2 THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 Information Security

Information security refers to the term that enables to protect the computer system from unauthorized access, use, disclosure, harassment, modification or destruction 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) means that data and information represented by data must be protected in such a way that use is limited only to authorized persons.

Integrity (I) means to protect users from unauthorized modification of information. Warranty that data will not be altered without proper authorization.

Availability (A) means that protecting users from unauthorized use of denial.

2.2 Cloud Computing

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 summarised as: (1) Private cloud (or In-house), where the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers; (2) Community cloud, where the cloud infrastructure provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns; (3) Public cloud, where The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them; and (4) Hybrid cloud, where the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

Companies that was using the cloud computing reported that cloud computing eanble to cut cost up to 30 percent, along with the another improve benefits, such as effective mobile working, higher productivity, and standardization of the process[25]. However this many benefits provided by the cloud computing, also accompanied by the introduction of the new risks[26,27], so there was a need in security requirement and management for cloud computing[27,28].

2.3 Security in Cloud Computing

Security and the privacy issues in cloud computing has received extensive attentions recently[29]. Scholars summarised the cloud into two categories: (1) cloud storage security, and (2) cloud computation security.

Cloud storage security referred to ensure the integrity of data stored at cloud servers while Cloud computation security refers to check the correctness of the computation performed by cloud servers[29].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 & Legalty.

Various framework and reccomendation 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 CyberSecurity framework, e.g. NIST CyberSecurity Framework[33,34]. This research tried to evaluate and incorporate the popular information security framework ISO27k series with the emerging CyberSecurity and IT Governance framework, the COBIT 5 for CyberSecurity.

2.4 ISO 27k Series & COBIT 5 CyberSecurity

International Standards for management systems provide models to set up and operate management systems, known as the standard of Information Security Management System (ISMS)[18].

The ISMS standard family consists of interrelated standards, already published or under development, and contains several significant structural components. ISO / IEC 27001 is the most recognizable standard in the family that provides the requirements for an information security management system (ISMS).

2.4.1 ISO 27001:2013

ISO 27001:2013 provides normative requirements for the development and operation of information security, including a set of controls for risk control and mitigation associated with information assets that the organization wishes to protect by the operation of information security[18].

Structurally, ISO 27001:2013 is divided into 2 major parts:

- Clause, is a condition that requirements must be met if the organization implements information security using ISO 27001:2013 standards
- Annex A, is a reference document used as a guide in determining the security controls that must be implemented into the ISMS. In ISO 27001:2005, Annex A consists of 11 domain groups, 39 control objectives, and 133 controls, whereas in the amendment, ISO 27001:2013, Annex A consists of 14 domain groups, 35 control objectives and 114 controls.

2.4.2 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 *1*.

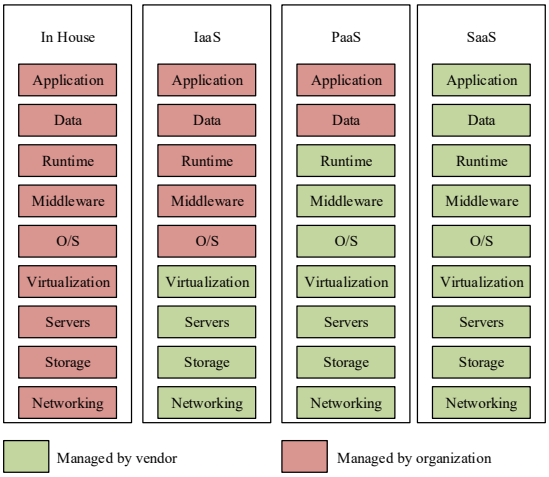

Figure 1 Organization and vendor's responsibilities in cloud computing, adopted from [35]

Based on the same research, it is also known that from 114 controls that exist in ISO 27001:2013, 102 effective controls are applied in private cloud computing without any significant depreciation.

2.4.3 COBIT 5

Control Objectives for Information and Related Technologies, commonly referred to as COBIT, is a best practice framework produced by ISACA for IT governance and management.

COBIT 5, which is issued by ISACA in 2012, provides a comprehensive framework that helps enterprise to create optimal value from IT by maintaining the balance between benefit, risk level, and resource usage[13]. COBIT 5 is a generic and useful guidance for enterprises of all sizes, whether commercial, non-profit, or public sector.

COBIT 5 framework offers a comprehensive set of publications, including the professional guides on several aspects and implementation as shown in Figure 2.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

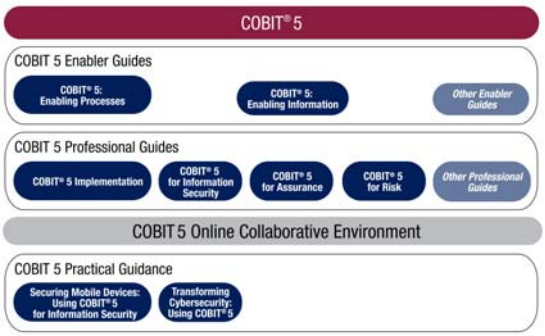

Figure 2 COBIT 5 Product Family, adopted from [19]

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 Cybersecurity Using COBIT 5*. In this paper, author focused on the latter, based on COBIT 5 for CyberSecurity[19].

2.4.4 COBIT 5 for Cybersecurity

Cybersecurity 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 Cybersecurity. COBIT 5 for Cybersecurity divided into several processes: (1) Cybersecurity Governance; (2) Cybersecurity Business Case; (3) Applying to Cybersecurity; (4) Cybersecurity Management; and (5) Cybersecurity Monitoring. This paper use the third process, Applying to Cybersecurity Process, which description can be seen in Table 1.

Table 1 COBIT 5 Applying to Cybersecurity Processess, 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 infromation 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
DSS05.05	Manage physical access to IT assets
DSS05.06	Manage sensitive documents and output services
DSS05.07	Monitor the infrastructure for security-related events

2.5 Maturity Level Framework

2.5.1 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].

2.5.2 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organizational process. Achieving each level of maturity forms a different component of the organizational process, which indicates a more mature and capable information system.

In its development, the Maturity Levels used in SSE-CMM contained in ISO 21827:2008 are replaced with maturity levels based on ISO 15504, particularly in the assessment of system maturity levels based on ISO 15504-6:2013[40]. In ISO 15504-6:2013, the maturity level is called the capability level.

This research uses a maturity index based on previous research[11] and the capability level and definition of ISO 15504-6: 2013 as reference[41]. Details of the calculation of the value of the maturity level with the index of maturity to obtain the level of maturity could be seen in Table 3.

Table 3 Maturity Level Assessment Criteria Index, adopted from [11,41,42]

Maturity Index	Maturity Level
0 – 0.49	0 – Incomplete
0.51 – 1.50	1 – Performed
1.51 – 2.50	2 – Managed
2.51 – 3.50	3 – Established
3.51 – 4.50	4 – Predictable
4.51 – 5.00	5 – Optimised

This maturity level is made in the form of nominal rank sizes to sort the maturity of the immature to the most mature. The definition of each level of maturity can be seen in Table 4.

Table 4 Maturity Level Definition, adopted from [41]

Maturity Level	Definition
0 – Incomplete	Not implemented or little or no evidence of any systematic achievement of the process purpose
1 – Performed	Process achieves its process purpose
2 – Managed	Implemented in a managed fashion (planned, monitored, and adjusted) and its work products are appropriately established, controlled, and maintained
3 – Established	Implemented using a defined process that can achieve its process outcomes
4 – Predictable	Operates within defined limits to achieve its process outcomes
5 – Optimised	Continuously improved to meet relevant current and projected enterprise goals.

3 METHODOLOGY

In this research, the authors used quantitative and qualitative research methods to find the immature part of University XYZ's cloud computing and provide recommendations to develop the conditions of the organization based on these findings. The steps used in this study can be seen in Figure 3.

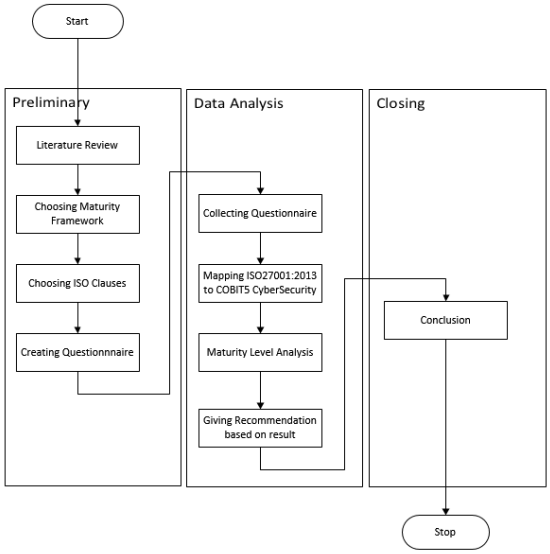

Figure 3 Research Methodology, adopted from [11]

3.1 Data Collection

This research uses questionnaires in its data collection. Question on this questionnaires is adopted from the compliance checklist provided by the Integrated Assessment Services / IAS[43]. The data provided by the respondent is processed with and processed by using Excel application. Based on the 12 questionnaires distributed to the IT department at University XYZ, this research received 11 respondents from the IT department with functional structure that can be seen in Table 5.

Table 5 Research Respondent

Functional Structure of IT Department in University XYZ	Amount
IT Manager	1
IT Support	3
Programmer	4
Network Engineer	2
Helpdesk	1

Based on the data that has been filled in the questionnaire, the next step is data analysis based

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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.

3.2 Mapping ISO27001:2013 to COBIT 5 for CyberSecurity

The basic difference between COBIT 5 for CyberSecurity and ISO27001:2013 was that ISO27001:2013 focused only on information security and COBIT 5 for CyberSecurity is focused on IT Governance with additional control for CyberSecurity. Thus, COBIT 5 for CyberSecurity 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 CyberSecurity by using COBIT 5 for CyberSecurity in a new mapping model.

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

For the mapping of these frameworks, every COBIT 5 for CyberSecurity section Applying to CyberSecurity 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 CyberSecurity processess can be seen in Table 6.

Table 6 Mapping of COBIT 5 for CyberSecurity to ISO27001:2013

COBIT 5 CyberSecurity (Applying to CyberSecurity) 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
APO13.02	Define and manage and information security risk treatment plan	A.6.1	Internal organization
		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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	services	A.8.2	Information classification
		A.8.3	Media handling
DSS05.07	Monitor the infrastructure for security-related events	A.12.4	Logging and monitoring

3.3 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.

3.3.1 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.

3.3.2 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.

3.3.3 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.

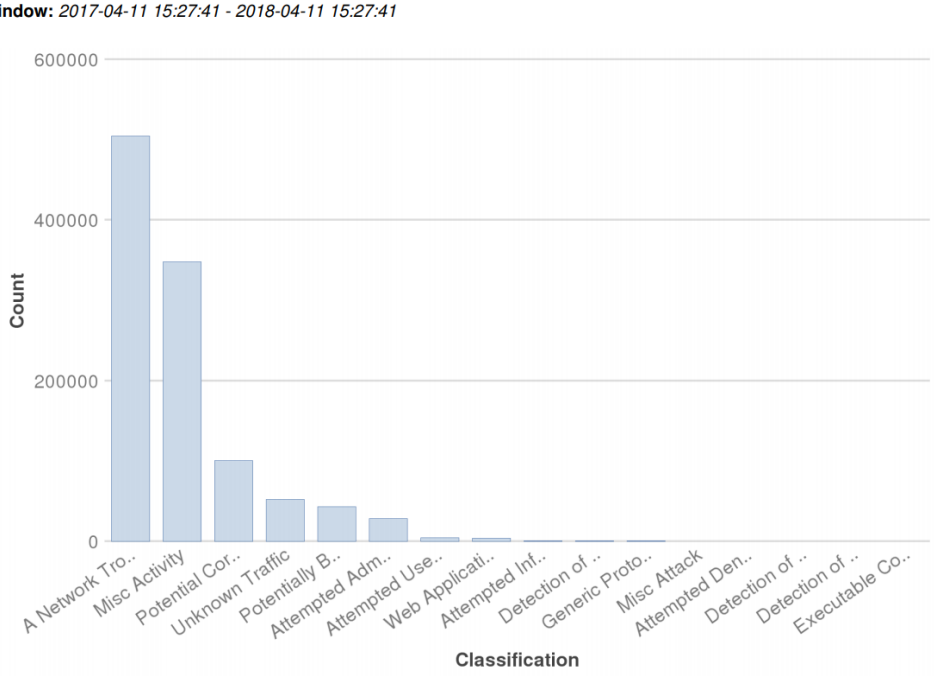

Figure 4 Intrusion event and its classification

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4 FINDINGS AND STRATEGY FOR INFROMATION SECURITY

4.1 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 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.

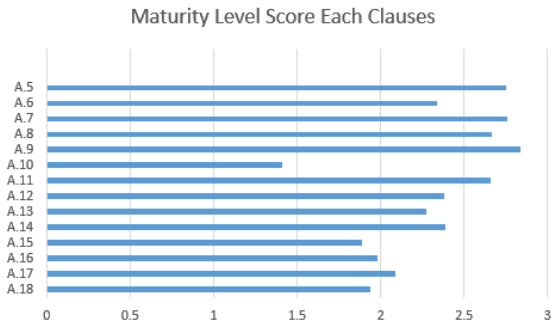

Figure 5 Graph of Maturity Level Score for Each Clause

Based on this result and the mapping reference from COBIT5 for CyberSecurity process to ISO27001:2013, Maturity level for COBIT5 for CyberSecurity process can be seen in Table 8.

Table 8 Maturity level of CyberSecurity 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 CyberSecurity appliance of private cloud computing at University XYZ is 2.44. This value indicates that the CyberSecurity 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 CyberSecurity process, a graph of maturity level can be seen in Figure 6.

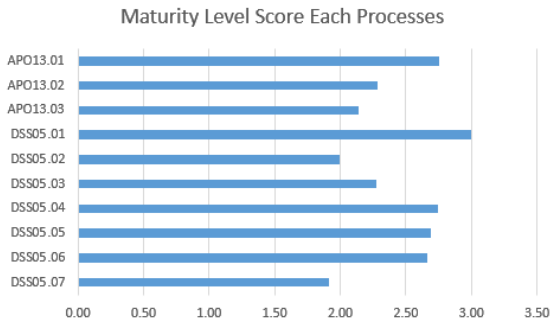

Figure 6 Graph of Maturity Level Score for Each Process

4.2 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 CyberSecurity 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of University XYZ (> 5 years) and the expectations of the University's stakeholder and the IT Manager who want good information security and CyberSecurity 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	Expected 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

Table 10 Maturity Level CyberSecurity Gap Analysis

Process	Current Score	Expected 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 (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 CyberSecurity 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 CyberSecurity 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 CyberSecurity processes that exist.

It is necessary to look for minimal / weak ISO control and COBIT5 for CyberSecurity 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.

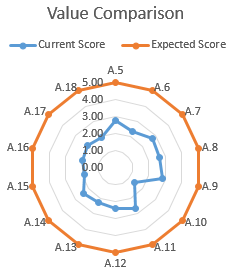

Figure 7 Ratio Value Between Current Maturity Level and Expectations (ISO27001:2013)

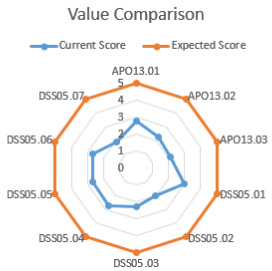

Figure 8 Ratio Value Between Current Maturity Level and Expectations (COBIT5 for CyberSecurity)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From Figure 7, it is known that Annex A.10 (Cryptography) has the lowest value with current maturity level and gap of 1.41 and 3.59, followed by Annex A.15 (Supplier relationships) of 1.89 and 3.11, and Annex A.18 Compliance for 1.94 and 3.06. These findings are summarized as Table 11.

Table 11 Highest Gap (ISO27001:2013)

No	Lowest Score	Gap	Annex No (Clauses)	Control Name
1	1.41	3.59	A.10	Cryptography
2	1.89	3.11	A.15	Supplier relationships
3	1.94	3.06	A.18	Compliance

It is also known that Annex A.9 (Access control) has the highest score of 2.84 and 2.16, Annex A.7 (Human resource security) of 2.76 and 2.24, and Annex A.5 (Information security policies) of 2.75 and 2.25. These findings are summarized as Table 12.

Table 12 Lowest Gap (ISO27001:2013)

No	Highest Score	Gap	Annex No (Clauses)	Control Name
1	2.84	2.16	A.9	Access control
2	2.76	2.24	A.7	Human resource security
3	2.75	2.25	A.5	Information security policies

From Figure 8, it is known that Process DSS05.07 (Monitor the infrastructure for security-related events) has the lowest value with current maturity level and gap of 1.91 and 3.09, followed by DSS05.02 (Manage network and connectivity security) of 1.99 and 3.01, and APO13.03 (Monitor and review the ISMS) for 2.14 and 2.86. These findings are summarized as Table 13.

Table 13 Highest Gap (COBIT5 for CyberSecurity)

No	Lowest Score	Gap	Process	Process Name
1	1.91	3.09	DSS05.07	Monitor the infrastructure for security-related events
2	1.99	3.01	DSS05.02	Manage network and connectivity security
3	2.14	2.86	APO13.03	Monitor and review the ISMS

It is also know that DSS05.01 (Protect against malware) has the highest score of 3.00 and 2.00, APO13.01 (Establish and maintain an information security management system (ISMS)) of 2.75 and 2.25, and DSS05.04 (Manage user identity and logical access) of 2.74 and 2.26. These findings are summarized as Table 14.

Table 14 Lowest Gap (COBIT5 for CyberSecurity)

No	Highest Score	Gap	Process	Process Name
1	3.00	2.00	DSS05.01	Protect against malware
2	2.75	2.25	APO13.01	Establish and maintain an information security management system (ISMS)
3	2.74	2.26	DSS05.04	Manage user identity and logical access

4.3 Gap Analysis Discussion

From this gap analysis it is known that the higher the gap value, the more it shows that the clause in the ISO27001:2013 and the process in COBIT5 for CyberSecurity will have a greater probability of a security breach, and vice versa, if the value of the lower gap, will have a probability of a smaller breach of security.

This preliminary audit also shows that the weaknesses of some policies and sectors in private cloud computing which already implemented by University XYZ. With this preliminary audit and with the recommendations provided, XYZ University is expected to strengthen existing policies and sectors within existing private cloud computing, thus reducing known intrusion events.

4.4 Evaluation & Recommendation

Based on the analysis that has been done on University XYZ IT department, the value of existing findings will be adjusted to the security conditions of private cloud computing information based on ISO 27001:2013 and COBIT5 for CyberSecurity, section Applying CyberSecurity,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 CyberSecurity, 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 CyberSecurity condition to the expected value is 2.69 and 2.56. Based on this, it can be drawn the existing information security and CyberSecurity 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.

4.5 Future Work

This preliminary information security audit on private cloud computing is still using ISO 27001:2013 and COBIT5 for Security, Applying CyberSecurity 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 CyberSecurity to further integrate not only the ISMS, but also the IT Governance.

5 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 from attack.

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 CyberSecurity framework to analyze and assess the use of information security and identify the cybersecurity 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 cybersecurity 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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:http://www.sei.cmu.edu/library/assets/whitepapers/.

[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/S2212-5671(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. Annu Rev Econom 2010;2:395–424. doi:10.1146/annurev.economics.102308.124433.

[7] Wagstaff K, Sottile CA. Cyberattack 101: Why Hackers Are Going After Universities. NBC News 2015. https://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821 (accessed March 21, 2018).

[8] Harris CE, Hammergen LR. Higher education's vulnerability to cyber attacks. Univ Bus Mag 2016. https://www.universitybusiness.com/article/0816-wisp (accessed March 20, 2018).

[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 J Comput Appl 2016;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] Cartlidge A, Hanna A, Rudd C, Ivor M, Stuart R. An introductory overview of ITIL V3. 2007. doi:10.1080/13642818708208530.

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

[17] 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.

[18] 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 Http//Www 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.

[25] Bradshaw D, Folco G, Cattaneo G, Kolding

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

M. Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take. SMART 2011 / 0045 D4 – Final Rep 2012:1–82.

[26] Rebollo O, Mellado D, Fernández-Medina E, Mouratidis H. Empirical evaluation of a cloud computing information security governance framework. Inf Softw Technol 2015;58:44–57. doi:10.1016/j.infsof.2014.10.003.

[27] Chou DC. Cloud computing risk and audit issues. Comput Stand Interfaces 2015;42:137–42. doi:10.1016/j.csi.2015.06.005.

[28] Hamlen K, Kantarcioglu M, Khan L, Thuraisingham B. Security Issues for Cloud Computing. Int J Inf Secur Priv 2010;4:36–48. doi:10.4018/jisp.2010040103.

[29] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, et al. Security and privacy for storage and computation in cloud computing. Inf Sci (Ny) 2014;258:371–86. doi:10.1016/j.ins.2013.04.028.

[30] Fernandes DAB, Soares LFB, Gomes J V., Freire MM, Inácio PRM. Security issues in cloud environments: a survey. Int J Inf Secur 2014;13:113–70. doi:10.1007/s10207-013-0208-7.

[31] Ali M, Khan SU, Vasilakos A V. Security in cloud computing: Opportunities and challenges. Inf Sci (Ny) 2015;305:357–83. doi:10.1016/j.ins.2015.01.025.

[32] Yulianto S, Lim C, Soewito B. Information security maturity model: A best practice driven approach to PCI DSS compliance. Proc - 2016 IEEE Reg 10 Symp TENSYMP 2016 2016:65–70. doi:10.1109/TENCONSpring.2016.7519379.

[33] Chang V, Kuo Y-H, Ramachandran M. Cloud computing adoption framework: A security framework for business clouds. Futur Gener Comput Syst 2016;57:24–41.

[34] Shackelford S, Proia A, Martell B, Craig A. Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices 2014.

[35] Tariq MI, Santarcangelo V. Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing. Proc 2nd Int Conf Inf Syst Secur Priv (ICISSP 2016) 2016:201–8. doi:10.5220/0005648702010208.

[36] Jacobs PC, von Solms SH, Grobler MM. Towards a framework for the development of business cybersecurity capabilities 2016;7:51–61. doi:10.13140/RG.2.1.5110.0406.

[37] Ferraiolo K. The Systems Security Engineering Capability Maturity Model 1998.

[38] ISO/IEC. ISO/IEC 21827:2008(E) Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®). Int Organ Stand ISO 2008.

[39] Paulk MC, Curtis B, Chrissis MB, Weber C V. Capability Maturity Model for Software , Version 1 . 1. Carnegie Melon Univ 1993:82.

[40] ISO/IEC. ISO 15504-6:2013 Information technology — Process assessment — Part 6: An exemplar system life cycle process assessment model. ISOOrg [Online] 2013.

[41] Barnier B. COBIT 5. ISACA 2012.

[42] Krisanthi GAT, Sukarsa IM, Agung Bayupati IP. Governance audit of application procurement using COBIT framework. J Theor Appl Inf Technol 2014;59:342–51.

[43] IAS. Iso 27001 : 2013 Compliance Checklist Iso 27001 : 2013 Compliance Checklist 2013.