# Certificate of Appreciation

This is to certify that

**WIYLI YUSTANTI**

has participated as

**A Paper Presenter**

entitled

SELF ASSESSMENT OF INFORMATION SECURITY INDEXES AT THE STATE UNIVERSITY OF SURABAYA USING ISO/IEC 27001

in The 4th Consortium of Asia Pacific Education University (CAPEU)
International Conference on Science, Technology, Engineering, and Mathematics (STEM)
**"Innovation for Human Talents"**

at Rektorat Building, Universitas Negeri Surabaya, Indonesia
on May 22th-23rd, 2017

President of CAPEU

**Y.Bhg. Prof. Dato' Dr. Mohammad Shatar Sabran**

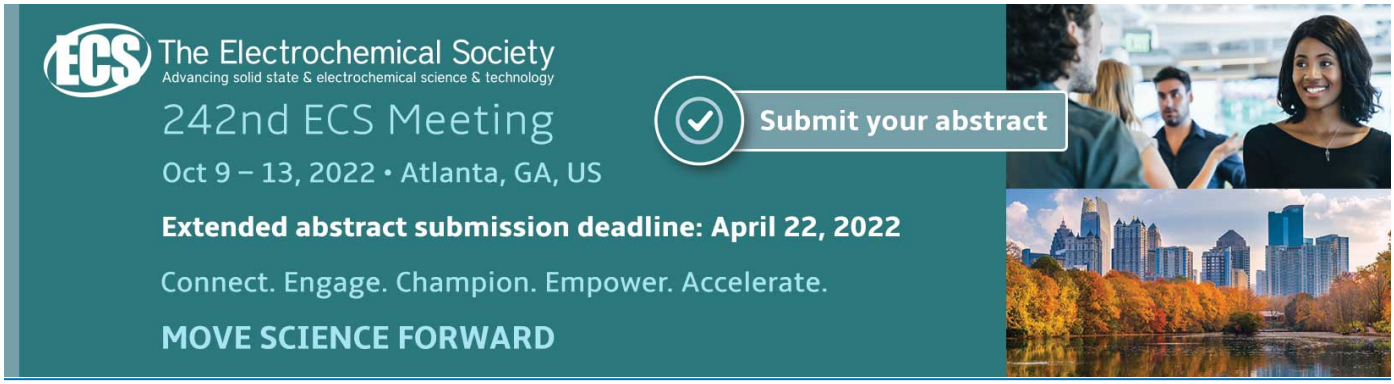
Rector of Unesa

**Prof. Dr. Warsono, M.S.**

http://capeu.conference.unesa.ac.id/

# The Consortium of Asia-Pacific Education Universities (CAPEU)





IOP Conf. Series: Materials Science and Engineering **296** (2017) 011001 doi:10.1088/1757-899X/296/1/011001

# Preface of
# The 4th CAPEU Conference 2017

The 4th Consortium Asia-Pacific Education Universities (CAPEU) 2017 is one of a series of international conferences held by Universitas Negeri Surabaya (Unesa), Indonesia, in collaboration with some universities in Asia, South East Asia, and Pacific as well as with other institutions. Unesa held this event as its commitment to research activities and collaborations to strengthen the academic climate in Asia and beyond. This event is a perfect platform for senior and junior researchers in the fields of sciences, technology, engineering, and mathematics to exchange experiences and ideas and to build a network. In addition, this conference will certainly help improve scientific publication of researchers and lecturers.

The theme of this year event is "Innovations for Human Talents". This two-day conference aims to bring together educators, graduate students, researchers, and faculty members of the CAPEU and of other countries to contribute to the concept of the STEM in education and to formulate goals on how this can be applied and implemented in their respective countries. The researchers can do their bit with their research findings in promoting better achievement of research innovation for the betterment of human life.

This conference has attracted much attention from scientific communities from diverse background of research interests. There are 130 research-based papers submitted and presented at the conference. Out of the submitted papers, the selected ones, around 56 papers, will be published by IOP Publishing. The papers have a wide range of topics, namely education, teaching and learning, assessment, community engagement, job opportunities related to STEM, and parents' involvement in enhancing STEM. The topics are not limited to, but mostly of the above-mentioned areas of interest.

**Editors:**

1. Abadi (Universitas Negeri Surabaya)
   abadi@unesa.ac.id
2. Ali Mustofa (Universitas Negeri Surabaya)
   alimustofa@unesa.ac.id
3. Setya Chendra Wibawa (Universitas Negeri Surabaya)
   setyachendra@unesa.ac.id

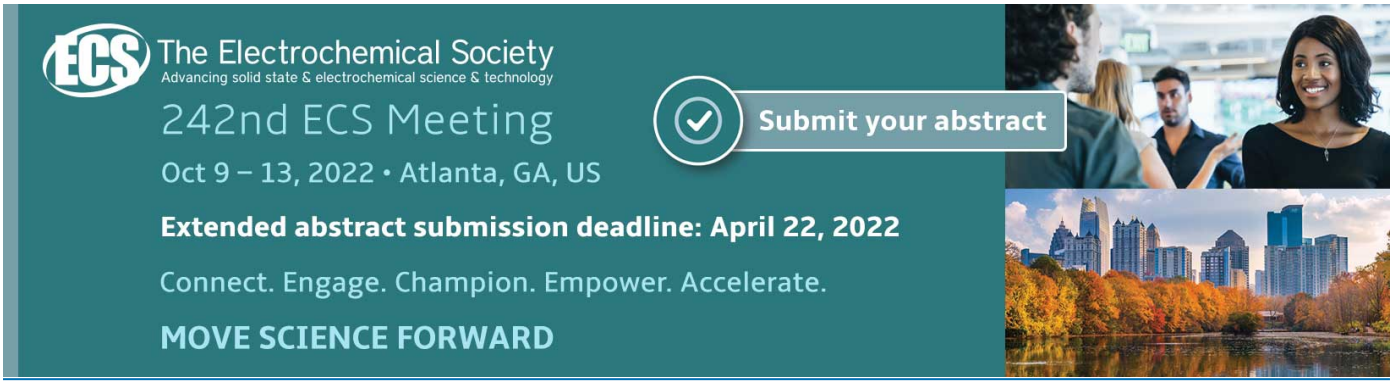
**Organize Commitee:**

Abadi (Universitas Negeri Surabaya)
Ali Mustofa (Universitas Negeri Surabaya)
Setya Chendra Wibawa (Universitas Negeri Surabaya)
Raya Sulistyowati (Universitas Negeri Surabaya)
Noviyanti (Universitas Negeri Surabaya)
Yuni Lestari (Universitas Negeri Surabaya)
Dimas Avian Maulana (Universitas Negeri Surabaya)
Muhamad Ro'is Abidin (Universitas Negeri Surabaya)

# Peer review statement

To cite this article: 2018 *IOP Conf. Ser.: Mater. Sci. Eng.* **296** 011002





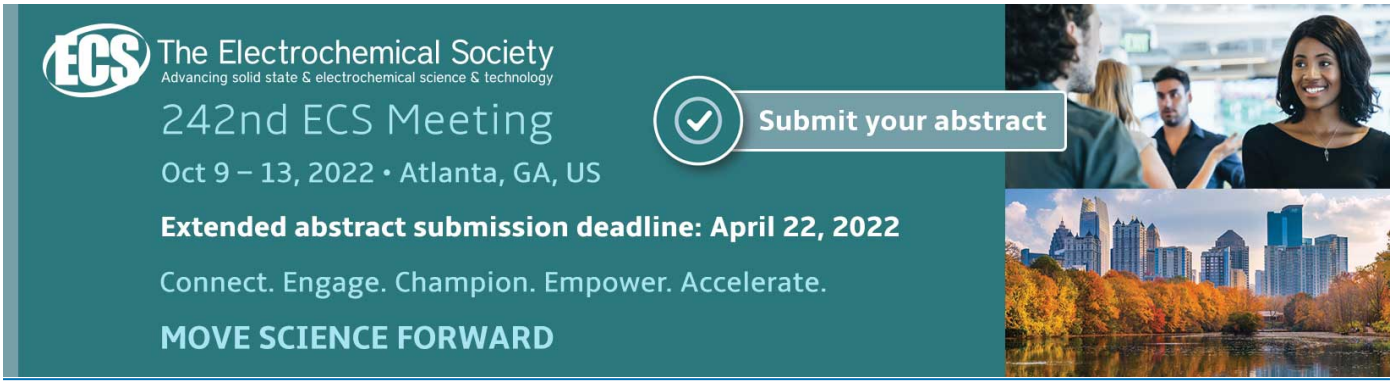
IOP Conf. Series: Materials Science and Engineering **296** (2018) 011002 doi:10.1088/1757-899X/296/1/011002

# Peer review statement

All papers published in this volume of *IOP Conference Series: Materials Science and Engineering* have been peer reviewed through processes administered by the proceedings Editors. Reviews were conducted by expert referees to the professional and scientific standards expected of a proceedings journal published by IOP Publishing.

# An analysis of Indonesia's information security index: a case study in a public university





IOP Conf. Series: Materials Science and Engineering **296** (2018) 012038 doi:10.1088/1757-899X/296/1/012038

# An analysis of Indonesia's information security index: a case study in a public university

**W Yustanti, A Qoiriah, R Bisma, A Prihanto**

Informatics Engineering Department, Universitas Negeri Surabaya, Indonesia

wiyliyustanti@unesa.ac.id

**Abstract**. Ministry of Communication and Informatics of the Republic of Indonesia has issued the regulation number 4-2016 about Information Security Management System (ISMS) for all kind organizations. Public university as a government institution must apply this standard to assure its level of information security has complied ISO 27001:2013. This research is a preliminary study to evaluate the readiness of university IT services (case study in a public university) meets the requirement of ISO 27001:2013 using the Indonesia's Information Security Index (IISI). There are six parameters used to measure the level of information security, these are the ICT role, governance, risk management, framework, asset management and technology. Each parameter consists of serial questions which must be answered and convert to a numeric value. The result shows the level of readiness and maturity to apply ISO 27001 standard.

## 1. Introduction

Currently, the implementation of Information and Communications Technology (ICT) governance is an obligation and demand for every organization of public service providers. The improving service quality as the realization of good governance is increasingly very important. The performance of organizational governance will be disrupted if information on ICT governance experiences security concerns that convey confidentiality, integrity, availability and non-repudiation. Guarantees to the security of ICT should refer to a standard that has been recognized by both national and international. There are various standards on information security, one of which is internationally recognized ISO / IEC 27001 in terms of the Information Security Management System (ISMS).

Public university as a government's organization must comply with government's regulations related to information security. This research investigates the completeness and the maturity level of information security in a public university in Surabaya. The methodology which used will explain the implementation of Indonesia's Information Security Index clearly. The results of the analysis of this study will be used to improve the organization's governance related to the security of information at a state university, especially the state university as a public service agency.

## 2. Information Security Management System (ISMS)

The Information Security Management System (ISMS) includes of rules, processes, guiding principle, and related assets and actions, which are accomplished communally by an organization, in order to guard its information stuff. The ISMS is a well-ordered methodology for building, applying, operating, checking, appraising, sustaining and refining the security of organizational information to accomplish

business goals. It is constructed by risk valuation and acceptance level of organizational risk considered to effectively handle and manage the risk. The success of an ISMS's implementation depends on analysis of requirements for applying proper controls to assure the protection of the information assets. The following basic rules also support the successful implementation of ISMS [1]:

- Awareness of the importance of information security
- The assignment of who is responsible for information security
- Management and stakeholder commitment to information security
- Improvement of social values
- Risk assessment that decides proper controls to gain acceptable levels of risk
- Security becomes an important part of information and systems networks
- Prevention and detection of active information security incidents
- Assure an overall approach to information security management
- Continual review of information security and the creation of proper modifications

### *2.1. ISO/IEC 27001*

ISO (*International Organization for Standardization*) and IEC (*International Electrotechnical Commission*) have published International Standards for the management system. The standard describes the steps to be followed in setting up and operating the management system. This procedure is a combination of features in which field experts have reached consensus internationally.

One of the standards issued related to information security is ISO / IEC 27001: 2013, published in September 2013 which is a replacement of ISO / IEC 27001: 2005. ISO / IEC 27001 is the result of a discussion of the Joint Technical Committee of ISO / IEC JTC 1 (*Information Technology*) and subcommittee SC 27 (*IT Security Techniques*). Members of ISO or IEC participate and collaborate in the development of International Standards through technical committees organized by each organization with specific topics of common interest [2].

### *2.2. Indonesia's Information Security Index (IISI)*

In Indonesia, the government adopted the ISO/IEC 27001:2005 to protect the public organization from information security risk. Ministry of Communication and Informatics of the Republic of Indonesia has issued the regulation number 4-2016 about Information Security Management System (ISMS). The law states that ISMS is an obligation for all organization which are processing their transaction using an electronic system based on risk principles.

The rule defines information security is a maintenance of confidentiality, integrity, and availability of information. The tool which is used to evaluate and analyse the degree of information security preparedness in an organization is mentioned as the Information Security Index (ISI).This method is published officially by National Standardization Agency with number SNI-27001.There are five domains to describe the level of information security based ISI standard[3]:

- *Information Security Governance*. This part evaluates the readiness of information security governance procedures and the agencies/functions, duties and responsibilities of information security executives.
- *Information Security Risk Management*. This part evaluates the readiness of implementing information security risk management as a basis for implementing an information security strategy.
- *Information Security Framework*. This part evaluates the completeness and readiness of the information security management (policy & procedure) framework and its implementation strategy.
- *Management of Information Assets*. This s part evaluates the completeness of safeguards against information assets, including the overall cycle of use of those assets.
- *Information Technology and Security*. This part evaluates the completeness, consistency and effectiveness of technology use in securing information assets.

The assessment process is then done through 2 (two) methods:

- The number (completeness) of the form of security. This method will evaluate the extent to which the respondent's institution has applied safeguards in accordance with the completeness of controls required by ISO / IEC 27001: 2009 standards.
- The maturity level of the information security management process. This method is an extension of the completeness evaluation and is used to identify the level of maturity of safeguard implementation with categorization that refers to the level of maturity used by the COBIT (*Control Objective for Information and Related Technology*) or CMMI (*Capability Maturity Model for Integration*) framework [4, 5].

Before the assessment process is done quantitatively, the role of ICT in the organization or scope must be evaluated first. The respondent will be asked to describe the existing ICT infrastructure in the organization briefly. The purpose of this process is to cluster the instance to a certain "size" i.e. Low, Medium, High and Critical. The categories of ICT Roles can be described as follows:

- *Minim.* The use of ICT in defined scope is insignificant, and its presence has no effect on the working process.
- *Low*. The use of ICT supports ongoing work processes, although not at a significant level.
- *Medium*. The use of ICT is part of the ongoing work process, but the dependency is still limited.
- *High*. ICTs are an integral part of the working process.
- *Critical*. The use of ICT is the only way to run a work process that is strategic or national scale.

## 3. Results and Comments

The methodology used for this study can be explained by steps such as Figure 1. The first step to do is to define the scope of the assessment. The scope of this research is the ICT Service Centre at a public university in Surabaya.

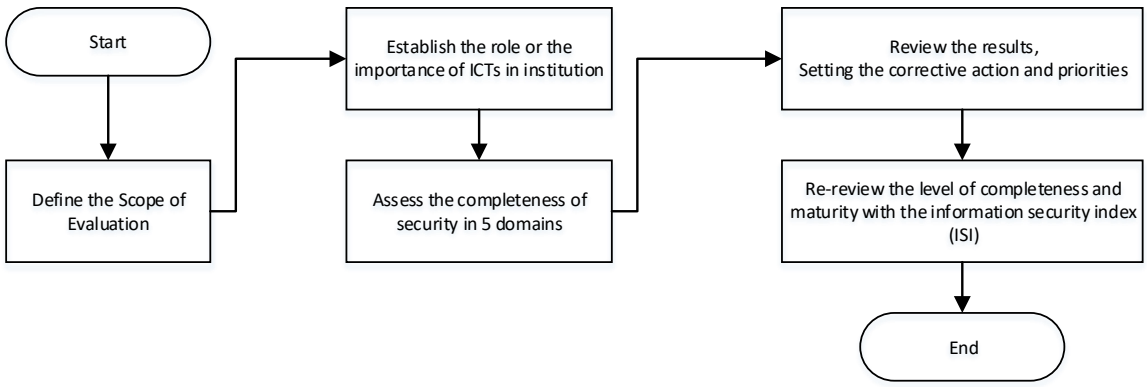



**Figure 1**. Procedure to evaluate the completeness and maturity level of information security indexes

The second step is to evaluate the role and the importance of ICT unit in the university. This activity will deliver a total score which describes how the dependence of organization on the ICT. The conclusions of the assessment can refer to table 1 that has been defined in the ISI index.

**Table 1.** Classification of ICT Role based on Total Score

| Range | Classification |
|---|---|
| 0 - 12 | Low |
| 13 - 24 | Medium |
| 25 - 36 | High |
| 37 - 48 | Critical |

By doing some interviews, the result of assessment can be described in table 2.

**Table 2.** Questions to evaluate the role of ICT in an organisation

| No | Questions | Answers | Scores |
|---|---|---|---|
| 1.1 | The total annual budget allocated to ICT:<br>● Less than IDR 1 Milliard = Minim<br>● IDR 1 Milliard up to IDR 3 Milliard = Low<br>● IDR 3 Milliard up to IDR 8 Milliard = Medium<br>● IDR 8 Milliard up to IDR 20 Milliard = High<br>● IDR 20 Milliard or more = Critical | Medium | 2 |
| 1.2 | The number of staff / users in institutions using infrastructure ICT :<br>● Less than 60 = Minim<br>● 60 to 120 = Low<br>● 120 to 240 = Medium<br>● 240 to 600 = High<br>● 600 or more = Critical | Critical | 4 |
| 1.3 | The level of dependence on ICT services to run the duties and functions of your institution | Critical | 4 |
| 1.4 | The value of intellectual property owned and produced by your institution | Low | 1 |
| 1.5 | The impact of major ICT system failures used by your institution | Critical | 4 |
| 1.6 | The level of dependence on the availability of ICT systems to connect the work location of your institution | Critical | 4 |
| 1.7 | The impact of your agency's ICT system failures on the performance of other government institutions or on the availability of national government systems | Critical | 4 |
| 1.8 | The level of sensitivity of ICT system users in your institution | Critical | 4 |
| 1.9 | The level of compliance with laws and other legal instruments | Medium | 2 |
| 1.10 | The potential loss or negative impact of incidents penetrated information security ICT system of your institution | Medium | 2 |
| 1.11 | The level of dependence on third parties in running/operating ICT systems | Low | 1 |
| 1.12 | The level of classification/criticality of ICT systems in your institution, relative to threats of attack effort or information security breach | Medium | 2 |
| | The importance of ICT role: | High | 34 |

The total score from Table 2 shows the number 34 if it refers to Table 1 can be said that the total evaluation score in the "High" category. It means that ICT is an integral part of the running work process. After knowing that the role of ICT in the university is very important then the next step based on figure 1 is to assess the completeness and maturity of information security. The assessment is done to 5 (five) domains. All questions in each area are grouped into 3 (three) categories of security, in accordance with the stages in the implementation of ISO / IEC 27001 standards. Questions related to

the basic information security framework fall under the category of "1", for the effectiveness and consistency of its application defined as categories "2", and those that refer to the ability to always improve information security performance are category "3". Table 3 shows the scoring of question answers.

**Table 3.** Classification of ISO 27001 Completeness

| Type of Answers (*implementation status*) | Completeness Category | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| are not done | 0 | 0 | 0 |
| in planning | 1 | 2 | 3 |
| in deployment or partially applied | 2 | 4 | 6 |
| are applied wholly | 3 | 6 | 9 |

Assessment is then done by analysing the number in each area and analysing whether the number has reached or exceeded the threshold of achieving a certain level of maturity. The calculation is done by applying the principle [4]:

- Achievement of maturity Level is done in accordance with the completeness and (*consistency and effectiveness*) of its implementation.
- A higher level of maturity requires the completeness, consistency and effectiveness of security at the lower levels.
- There is an additional level of maturity to provide a more detailed description, namely I +, II +, III +, and IV +, so that there are a total of 9 levels of maturity (figure 2).

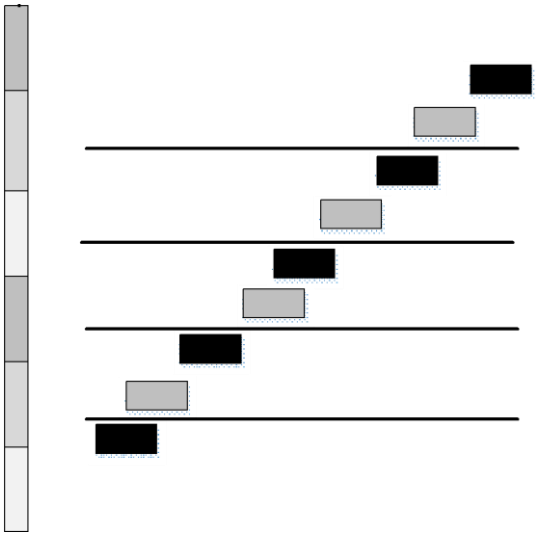


**Figure 2.** Levels of Maturity

In the information security scale based on the Information Security Index, the level of maturity is defined as follows:

- Level 0 : Unknown (*passive*)
- Level I : Initial Conditions (*reactive*)
- Level II : Implementation of the Basic Framework (*active*)
- Level III : Defined and Consistent (*proactive*)
- Level IV : Managed and Measurable (*continued*)
- Level V : Optimal Level (*optimal*)

Overall, the results of the assessment of the areas can be described in table 4.

**Table 4.** A Public University ICT Centre's Assessment Result

| Domains | Total Score | Maturity Level | Completeness Status | The number of questions based on completeness category | | |
|---|---|---|---|---|---|---|
| | | | | **1** | **2** | **3** |
| *Information Security Governance* | 58 | II | Valid | 8 | 6 | 6 |
| *Information Security Risk Management* | 40 | II | Valid | 9 | 4 | 2 |
| *Information Security Framework* | 27 | I+ | Not Valid | 11 | 8 | 7 |
| *Management of Information Assets* | 94 | II | Valid | 21 | 9 | 4 |
| *Information Technology and Security* | 75 | II | Valid | 13 | 10 | 1 |
| Total | 294 | | | | | |

The data in table 4 will be compared to ISO 27001 control in a radar chart.

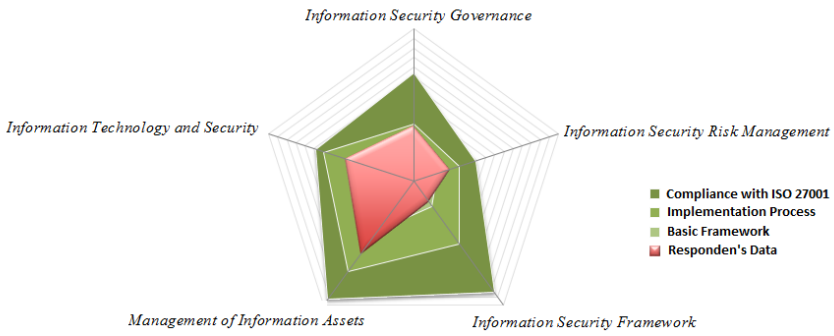



**Figure 3.** Completeness Level of 5 Domains in a Public University ICT Centre

In the radar diagram, the area background indicates the threshold level of completeness (category) 1 to 3 (light green to dark green).

**Table 5.** Correlation Matrix between Importance Level and Readiness Status

| ICT Role Score | ICT Role Classification | Total Score of 5 Areas IS Index | Readiness Status to ISO 27001 Standard |
|---|---|---|---|
| 0 - 12 | Low | 0 - 124 | Not Feasible |
| | | 125 - 272 | Need Improvement |
| | | 273 - 588 | Good/Enough |
| 13 - 24 | Medium | 0 - 174 | Not Feasible |
| | | 175 - 312 | Need Improvement |
| | | 313 - 588 | Good/Enough |
| 25 - 36 | High | 0 - 272 | Not Feasible |
| | | 273 - 392 | Need Improvement |
| | | 393 - 588 | Good/Enough |
| 37 - 48 | Critical | 0 - 333 | Not Feasible |
| | | 334 - 453 | Need Improvement |
| | | 454 - 588 | Good/Enough |

The value of each area is shown in the red area. In this diagram, can be seen the comparison between the conditions of readiness as a result of the evaluation process with reference to the level of completeness. The resulting quantities are then mapped in accordance with ICT's importance to the

scope of the organization based on the relationship matrix between the ICT level of importance and the total score (table 5). The analysis result from the respondent's data shows that the relationship between the total score (294) and the ICT's dependency (high category) conclude that the University ICT Centre still need improvement relate to Information Security. Table 5 illustrates that the higher the level of organizational dependence on ICTs or the more important the role of ICTs against the organization's work, then more forms of security are required and applied until it reaches the highest stage.

## 4. Conclusions

The conclusion that can be drawn from this study is that the level of readiness and maturity of the ICT unit at a state university in Surabaya in category II with a high level of dependence on ICT. This means:

- Security has been implemented even though most are still in the technical area and there is no linkage of security measures to obtain an effective strategy.
- The security process runs without documentation or an official recording.
- The operational safeguard measures applied depend on the knowledge and motivation of the implementing individual.
- The overall form of security has not been proven its effectiveness.
- Weaknesses in security management are still widely found and cannot be resolved thoroughly by the executor and the leader causing a very significant impact.
- Security management has not been prioritized and is not running consistently.
- The parties involved are likely to still not understand brand responsibility

For further study, the University ICT Centre needs detail correction in information security documentation, policy, and procedure in order to improve the maturity level to optimum status.

## References

[1] ISO/IIEC 2700, Information technology--Security techniques -- Information security management systems -- Overview and vocabulary, 4th edition, 15th Feb 2016
[2] ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements, https://www.iso.org/standard/54534.html, retrieved on 29th April 2017.
[3] Tim Direktorat Keamanan Informasi , Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (in Bahasa), 2011
[4] Covernace Institue 2017, Cobit 4.1 Framework Control Objectives Management Guidelines Maturity Models, , ISBN 1-933284-72-2 US.
[5] Junttila, Juho 2014. A Business Continuity Management Maturity Model, University of Turku