International Journal of Engineering & Technology, 9 (2) (2020) 429-436

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education

IGN Mantra [1] *, Aedah Abd. Rahman [2], Hoga Saragih [3]

[1] Dept. Informatics Engineering, Perbanas Institute, Jakarta, Indonesia
[2] School of Science and Technology, Asia e University, Subang Jaya, Malaysia
[3] Dept. Informatics Engineering, Bakrie University, Jakarta, Indonesia
**Corresponding author E-mail: ign.mantra@perbanas.id*

Abstract

Information Security Management System (ISMS) implementation in Institution is an effort to minimize information security risks and threats such as information leakage, application damage, data loss and declining IT network performance. The several incidents related to information security have occurred in the implementation of the Academic System application in Indonesian higher education. This research was conducted to determine the maturity level of information security practices in Academic Information Systems at universities in Indonesia. The number of universities used as research samples were 35 institutions. Compliance with the application of ISO 27001:2013 standard is used as a reference to determine the maturity level of information system security practices. Meanwhile, to measure and calculate the level of maturity using the SSE-CMM model. In this research, the Information System Security Index obtained from the analysis results can be used as a tool to measure the maturity of information security that has been applied. There are six key areas examined in this study, namely the role and importance of ICT, information security governance, information security risk management, information security management framework, information asset management, and information security technology. The results showed the level of information security maturity at 35 universities was at level 2 Managed Process and level 3 Established Process. The composition is that 40% of universities are at level 3, and 60% are out of level 3. The value of the gap between the value of the current maturity level and the expected level of maturity is varied for each clause (domain). The smallest gap (1 level) is in clause A5: Information Security Policy, clause A9: Access Control, and clause A11: Physical and environmental security. The biggest gap (4 levels) is in clause A14: System acquisition, development and maintenance and clause A18: compliance.

Keywords: *Information Security Management System; Information Security Maturity; ISO 27001:2013.*

1. Introduction

Academic Information System (AIS) is an application system created to realize the process of online academic activities. AIS is expected to be able to provide comprehensive and reliable information so that there is a need for comprehensive internal control that is able to maintain the AIS from various kinds of information security risks or threats such as information leakage, application damage, data loss, and declining performance of IT networks that support the AIS.

Information security in higher education AIS requires several approaches in its application. One application that can be done is to build controls that focus on aspects contained in security. The control in question is an internal control that emphasizes the interrelationship between business processes and security measures. At present there are several security control frameworks that can be used to build those controls [15]. One control that specifically puts forward the information security factor at present is ISO (International Organization for Standardization) 27001 [13].

ISO 27001:2013 is a standard for auditing the security of an information system and is used as a reference to produce documents (findings and recommendations). ISO 27001:2013 has 133 information security controls, and in practice companies can choose which controls are most relevant to conditions in the field [9]. But the selection is not an easy job, because many parameters must be taken into consideration. ISO 27001 has the advantage that this standard is very flexible which is developed depending on the needs of the organization, organizational goals, security requirements and also ISO 27001:2013 provides a certificate of implementation of a nationally and internationally recognized Information Security Management System called the ISMS [8].

1.1. Research problems

Academic Information System in almost all universities in Indonesia has been held online. Academic administration has been carried out through computer networks and the internet. These conditions can pose a risk problem for the security of information contained in a

Copyright © IGN Mantra et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

university's academic information system. The existence of a security gap in the system can be a major source of threat to the institution, which can affect the confidentiality, safety and availability of vital assets of the institution.
Besides, lack of awareness about the use of information technology in the way employees improperly handle information and technology - with or without intention - can cause damage that is not inferior to the previous one, especially when employees have access to high sensitivity data. such as student accounts and data and their academic records. Universities should have a special plan to protect information assets or reduce the risks that can threaten it. Therefore, universities need to improve their information security system programs in accordance with international standards. The initial step to achieve this is to assess the reality of information security practices based on information security governance standards such as ISMS. This measurement is intended to find out capabilities and gaps against internationally established governance standards.
From this research, several problems and questions will be formulated, namely:

a) What level do most universities in Indonesia practice information security based on ISMS information security governance standard?
b) How is the level of gap between the level of actual information security practices compared to the level to be achieved in accordance with the requirements of ISMS?
c) What domains and controls are the most vulnerable points that cause potential threats in Universities, and what solutions can be recommended to fix them?

1.2. Research objectives

This study aims to determine the extent of information security practices in most universities in Indonesia and assess the extent of their compliance with information security standards requirements. It is also an effort to measure the gap between the actual level of information security practices in higher educations and the level to be achieved in accordance with the requirements of ISMS. Besides, this study aims to find areas of control that represent practices that are in accordance with standards and also vulnerable points in security practices and provide recommendations needed to improve compliance with standards, reduce gaps and improve information security practices in Universities.

1.3. Research benefits

The significance of this research arises from the significance of the topics discussed, namely information security according to ISO 27001 standards. This is important because it highlights information security issues in various domains and controls, which are provided by this standard. Also important is the importance of information assets and their consequences if security breaches occur in institutions and systems. That becomes more significant in the environment under investigation (Some universities in Indonesia). This research will be beneficial for employees in IT Management in higher educations, and will contribute in raising awareness about how to deal with this problem so that it does not become a barrier that limits the efficiency of academic activities in higher educations.
Besides, this research is important because it increases understanding of managing information security assessments, ensuring proper information security management, which ensures business continuity. Information security is no longer a problem that is handled by each bureau or department separately. Instead, this is handled by decision makers at the leadership level which translates into policy and strategy.
In general, the benefits of this research are:

a) Provide an overview to university managers about the conditions and procedures that must be followed to improve the level of information security.
b) As a reference prepare a work plan for the application of international information security standards in higher education so that they can obtain an information security certificate.

2. Literature and information background

2.1. Information security

Information security can be interpreted as an effort to secure information assets from all kinds of threats that might occur to reduce the negative risk that is received. According to the definition of ISMS, information security is defined as maintaining the, integrity(I), confidentiality(C) and availability(A) of information; besides, the nature of other information such as authenticity, accountability, non-compliance and reliability can also be included.
Information security has several aspects which are the main concern that must be understood in its application. Some aspects are often understood as C.I.A triangle model which consists of confidentiality, integrity, and availability. Chad Perrin explained in "The CIA Triad" that information security should: (1) Guarantee that only those who have the right can access certain information (confidentiality), (2) It can be guarantee the completeness of information and protect against corruption, damage, or other threats that cause changes in information from the original (Integrity), and can guarantee users can access information at any time without interruption and not in a format that cannot be used (availability).
Meanwhile, information security can be threatened because people, organizations, mechanisms, or events that have the potential to jeopardize the company's information resources. Threats can be at internal or external and can be accidental or intentional (McLeod and Schell 2004, 244). The types of threats to the security of information systems also vary, both from within the organization and from outside. Types of threats to information security according to ISO 27005:2008 can be in the form of physical damage (fire, water, pollution); natural events (climate, seismic, volcanic); loss of important services (electric power, HVAC, telecommunications); information compromise (eavesdropping, taking of discarded materials, media theft); technical failure (equipment, capacity saturation, software); and compromise functions (abuse of rights, errors in use, denial of action. Meanwhile, if viewed from the classification of the origin of the threat, according to ISO 27005: 2008, the threat can be intentional for the purpose of espionage or processing of illegal data, accidental (software failure, equipment failure), environmental origin (natural events, loss of electricity supply), or negligence.

2.2. Academic information system

Academic Information System is an application software used to present administrative information related to academic activities. By using application software like this, it is expected that academic administrative activities can be managed well and the information needed can be obtained easily and quickly.
Academic Information System is a system that processes data and processes academic activities involving students, lecturers, academic administration, finance and other attribute data.
Academic information systems carry out student administrative processes in conducting academic administrative activities, carry out processes in teaching and learning transactions between lecturers and students, conduct academic administration processes both concerning the completeness of documents and costs incurred in registration activities or the daily operational activities of academic administration.
The process of financial data processing is done every time a financial transaction is carried out by a student, so that in this process the Academic Information System can update student data. Some parts related to the financial module can be integrated under the Academic Information System, the financial module can be in the form of accounting transaction activities or staffing transaction activities which are processes that occur in activities at the University or Academic.

2.3. Academic information system in Indonesian higher education

Academic information system is a system created to facilitate academic administration activities on campus, all of which are managed online. Some examples of administrative activities on campus are New Student Admissions (PMB), compilation of curriculum and class schedules, filling in Study Plan Cards (KRS), filling grades (for lecturers), managing data of lecturers, staff, and students, etc.
Excellence of Academic Information Systems:
Academic Information System (AIS) is designed to be able to process all existing information in an integrated manner, so that the available data is always up to date in real time.

Besides, because the database is centralized, AIS can minimize the duplication of data commonly found in manual systems.
AIS can function as an information center with advantages in the form of:

- Automatic email response
- Online New Students Admission
- Online Study Plan
- Online class scheduling
- Online assessment

Being the center of track record of all campus activities because all data is in AIS including the latest news about campus.
Communication media for lecturers, employees, and students.

Academic Information System can contain data:

- Student Data
- Lecturer Data
- Course Data.
- Study Plan
- Student Score List
- Student Graduation Data
- Financial Data

The data that can be accessed by AIS users are:

- Student names List
- Lecturers names List
- Course schedule
- Student Value List
- Student Present List
- Graduation Names List
- Active Students Data in Courses

Benefits of Academic Information System, make it easier for students to get information without having to come to the administration on campus which is often long because they have to queue, etc.
The campus administration section is also facilitated by the presence of AIS because it reduces the burden to interact with students who are in need of data. The administration section can focus its time on data input and data checking. Data is stored in a structured manner with a database stored on the computer. Data updating between the campus administration section and the finance department can be done quickly in realtime. More effective financial data processing using applications that can support financial processes and staffing processes.
AIS is very helpful in the academic process in Universities, so it is necessary to secure all data contained in the program, both lecturers, employees, administrative processes, finance and others. Here ISMS is very instrumental in securing a series of academic information systems.

2.4. ISMS ISO 27001:2013

International Standard ISO 27001:2013 is an international information security standard that contains requirements that must be met in an effort to use information security concepts that apply internationally to an organization [2].
This International Standard establishes requirements for the establishment, implementation, maintenance and improvement of an Information Security Management System (ISMS) in an organizational context on an ongoing basis. This standard also includes requirements

for the assessment and handling of information security controls that are tailored to the needs of the organization. These standard requirements are general in nature and are intended to be applied to all organizations regardless of type, size and nature [3].

The Clauses in ISO 27001: 2013 consist of 7 Clauses, namely:
1) Clause 4 Organizational Context
2) Clause 5 Leadership
3) Clause 6 Planning
4) Clause 7 Supporting
5) Clause 8 Operations
6) Clause 9 Performance Evaluation
7) Clause 10 Improvement

In ISO 27001: 2013 consists of:
14 Control Areas: core topic areas that discuss aspects of information security,
34 Control Objectives: Control Objectives,
114 Controls: Controls apply to be implemented in an Information Security Management System.

Table 1: List of Control Areas (Annex A)

No.	A	Annex Control Area
1.	A.5	Information Security Policy
2.	A.6	Organizational Information Security
3.	A.7	Security of human resources
4.	A.8	Asset Management
5.	A.9	Access Control
6.	A.10	Cryptographic
7.	A.11	Physical and environmental safety
8.	A.12	Security operations
9.	A.13	Security Communication
10.	A.14	System acquisition, development and maintenance
11.	A.15	Supplier Relationship
12.	A.16	Management of Information Security Incidents
13.	A.17	Security Aspects of Information of Business Continuity Management
14.	A.18	Compliance

2.5. Maturity level

The maturity level of information security implementation can be measured using the maturity model. Maturity model is a method to measure the level of process management development, which means is to measure the extent of the management's capabilities in implementing information security. There is good management development or capability depends on the achievement of the objectives of the ISMS has been implemented.

The Calculation model used to measure the level of maturity using SSE-CMM. SSE-CMM is a Capability Maturity Model (CMM) for System Security Engineering (SSE). CMM is a framework for developing processes, such as formal and informal technical processes. SSE-CMM consists of two parts, namely:
a) Model for the security of processes, projects and organizations.
b) Assessment methods to determine the maturity of the process.

Base on SSE-CMM, the level of IT management capabilities on a maturity scale is divided into 6 levels namely [8]:

Table 2: Maturity Level

Level	Description
Level 0	Incomplete Process. The process was not implemented or failed to reach the specified output.
Level 1	Performed Process. The process has been carried out and successfully achieved the goal.
Level 2	Managed Process. It has been implemented and implemented in a more orderly manner and the resulting outcomes have been well established, controlled and maintained
Level 3	Established Process. The process has been carried out according to the rules / processes set and is able to achieve the expected output.
Level 4	Predictable Process. The process has been implemented in accordance with predetermined rules to achieve the expected outcomes.
Level 5	Optimizing Existing processes on a regular and continuous basis are improved to achieve the expected goals both now and in the future

3. Methodology

The methodology used in this research is descriptive analytic method to analyze and identify compliance with international information security standards. Data and information from compliance with information security standards is used as a measure of the level of ability to implement information security practices. This data and information were collected from 35 universities spread throughout Indonesia.
In general, the steps taken in this study are:
1. Determine research objectives
2. Literature review
3. Design questionnaire questions used for data collection
4. Questionnaire data processing and analysis
5. Recommendations

Questions asked to respondents using the approach contained in 114 compliance controls in 14 domains required by ISO27001. The grades are determined by the requirements of security practices that have been applied at each college. Each control has several statements /

questions that will be converted to the level of maturity of the control implementation. The average value of several controls included in one domain, will be used as an index of maturity level. The maturity index will be used to determine the level of maturity level of each domain. The equivalent or relation is as shown in table 4.

Table 3: The Example Questionare Questions

A.11 Physical and environmental security	Score
Does the organization's data center have controls to ensure that the authorities physically access it?	4
Does the organization have various safeguards to protect critical hardware and cables from natural threats and human threats?	5
Does the organization have a process of issuing keys, codes and / or cards that require appropriate authorization and background checks for access to sensitive facilities?	4
Does the organization follow vendor-recommended guidelines for maintaining physical equipment?	3
Does the organization have a media sanitization process that is applied to a variety of equipment before being thrown into the trash, reused, or destroyed?	2
Are there a process of detecting removal of equipment, information or software without the organization's permission?	1
Maturity Index	3.17

Table 4: Index Matching with Maturity Level

Maturity Index	Maturity Level
0.00-0.50	0
0.51-1.50	1
1.51-2.50	2
2.51-3.50	3
3.51-4.50	4
4.51-5.00	5

Table 3 shows that the maturity index of Domain A.11 Physical and environmental security is 3.17. Based on table 4, the level of maturity of the implementation of the domain is at level 4.

4. Results

From the results of a survey that has been conducted will be analyzed regarding the level of maturity and gap analysis of information security practices based on ISMS.

4.1. Maturity level

From the survey conducted in this study, the results obtained as shown in table 4. From the data in table 4, the maturity level of each college is calculated, by calculating the average level of the entire clause (A5 to A18), to then convert to maturity level according to table 4. The results are as shown in Figure 1.

Table 5: Survey Result

University	Maturity Level of Clause ISO 27001: 2013													
	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
U1	4	2	2	4	5	3	4	4	3	2	2	3	2	1
U2	5	3	3	5	5	3	5	5	3	2	2	2	2	2
U3	5	3	3	5	5	3	5	5	3	2	2	2	2	2
U4	5	3	3	5	5	3	5	4	3	2	2	2	2	2
U5	5	3	3	4	5	3	4	4	3	2	2	2	2	2
U6	4	3	2	3	4	3	3	3	2	1	1	1	1	1
U7	3	2	2	3	3	2	3	3	2	1	1	1	1	1
U8	3	2	2	3	3	2	3	3	2	1	1	1	1	1
U9	4	3	2	3	3	2	3	3	2	1	1	1	1	1
U10	3	2	2	3	3	2	3	3	2	1	1	1	1	1
U11	5	2	3	4	4	3	4	4	3	2	2	2	2	2
U12	5	3	2	3	4	3	4	4	3	2	2	2	2	2
U13	5	2	3	3	4	3	4	4	3	2	2	2	2	2
U14	5	3	2	4	4	3	4	4	3	2	2	2	2	2
U15	5	3	3	3	4	3	4	4	3	2	2	2	2	1
U16	3	2	1	3	3	2	3	3	2	1	1	1	1	1
U17	3	2	1	3	3	2	3	3	2	1	1	1	1	1
U18	4	2	1	3	4	3	3	3	2	1	2	2	2	2
U19	3	2	1	3	3	2	3	3	2	1	1	1	1	1
U20	4	2	1	4	4	3	3	3	2	1	2	2	2	2
U21	3	2	1	3	3	2	3	3	2	1	2	2	2	2
U22	3	2	1	3	3	2	3	3	2	1	2	2	2	2
U23	3	2	1	3	3	2	3	3	2	1	2	2	2	1
U24	3	2	1	3	3	2	3	3	2	1	2	2	2	2
U25	3	2	1	3	3	2	3	3	2	1	2	2	2	2
U26	5	3	3	3	4	3	4	4	3	2	2	2	2	1
U27	3	2	1	3	3	2	3	3	2	1	1	1	1	1
U28	3	2	1	3	3	2	3	3	2	1	1	1	1	1
U29	4	3	2	3	4	3	4	4	3	2	1	1	2	1
U30	4	3	2	3	4	3	4	4	3	2	1	1	1	1
U31	3	2	1	3	3	2	3	3	2	1	2	2	2	2
U32	3	2	1	3	3	2	4	4	3	2	1	2	1	1
U33	5	3	2	4	4	3	4	3	2	1	2	2	2	1
U34	3	2	1	3	3	2	3	3	2	1	1	1	1	1
U35	3	2	1	3	3	2	3	3	2	1	1	1	1	1

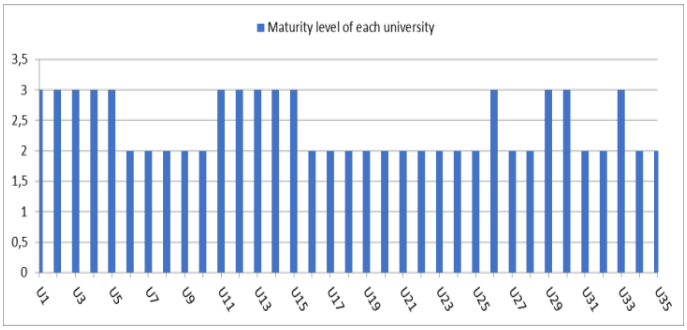

Fig. 1: Maturity Level of Each University.

The information shown in Figure 1 shows the level of maturity of the 35 universities surveyed. The maturity level is obtained by converting the average magnitude of the maturity level of all domains (A5 to A18) to the maturity index, and then correlated with the maturity level, according to table 4.
Based on the graphic images obtained information that the level of maturity is at level 3 Managed Process and level 4 Established Process. The composition of universities at level 3 is 40% of the total, the remaining 60%, this means that most universities in Indonesia have a maturity level of 2, so it can be concluded that the maturity level of information security practices at several universities in Indonesia is still low.

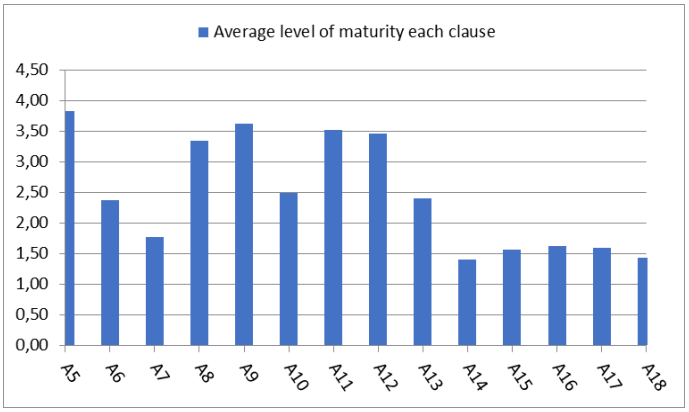

Fig. 2: Average Maturity Level Per Clause.

The results also show that there are several clauses that obtain a large level of maturity (above 3). This clause with maturity level is assumed that the security controls in the clause have been implemented well. There are 5 clauses that have a good level of implementation, namely:

1) A.5: Information Security Policy
2) A.8: Asset Management
3) A.9: Access Control
4) A.11: Physical and environmental safety
5) A.12: Security operations

4.2. Gap analysis

Gap Analysis is a comparison of actual performance with potential or expected performance. This method is an evaluation tool that focuses on current performance gaps with previously targeted performance. Gap analysis can be used to identify actions needed to reduce gaps or achieve expected performance, this analysis can be used to estimate the time, cost, and resources needed to achieve an expected situation (Jennings, M. D., 2000).

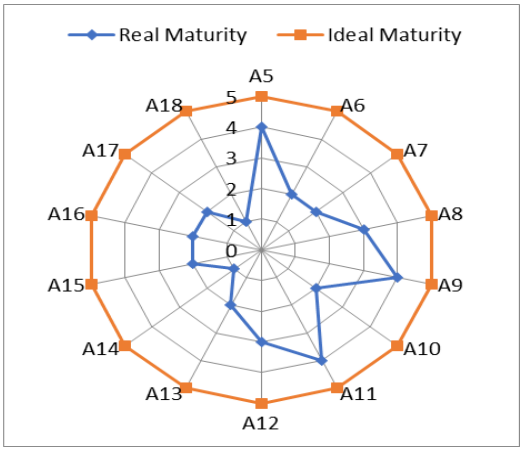

Fig. 3: Gap Level.

Based on Figure 2, it can be seen that the Information Security Policy Clause (A.5) has a maturity level of 4, the Information Security Organization Clause (A.6) has a maturity level of 2, the Human Resource Security Clause (A.7) has a maturity level of 2, Asset Management Clause (A.8) has a maturity level 3, Access Control Clause (A.9) has a maturity level of 4, Cryptographic Clause (A.10) has a maturity level of 2, Physical and Environment Security Clause (A.11) has a maturity level of 4, Security Operations Clause (A.12) has a maturity level of 4, Communication Security Clause (A.13) has a maturity level of 2, the Acquisition, Development and Improvement System Clause (A.14) has a maturity level of 1, Supplier Relationship Clause (A.15) has a maturity level of 1, the Information Security Incident Management Clause (A.16) has a maturity level of 2, and an Information Security Aspect Clause in Sustainability Management Business (A.17) has a maturity level of 2 and the last Compliance Clause (A.18) has a maturity level of 1.
From the description of the gap / gap, shows that there are some controls that have a gap that is close to ideal conditions and also some controls that have a gap that is far from the ideal condition.

The clauses that have a small gap are as follows:
1. A5: Information Security Policy
2. A9: Access Control
3. A11: Physical and environmental safety

The clauses that have the biggest gaps are as follows:
1. A14: System acquisition, development and maintenance
2. A18: Compliance

In general, there are no controls that are fully implemented with a 100% compliance level (at level 5), nor are there full controls that are not carried out at all (level 0).
Based on the domain of institutional fulfillment, it can be seen that most universities do not meet the ISMS clause on the control of system acquisition, development, and maintenance (A.14). This is due to the fact that several universities do not have adequate security policies towards the development and development of information systems, both in terms of software and hardware. When an institution develops a related system, most do not include data and information security agreements between the institution and the system developer.
Besides, the majority of universities also do not meet compliance controls (A.18). This compliance control is related to the audit process both internal and external.

5. Conclusion

The Maturity level of information security practices in higher education academic information systems in Indonesia is at level 2 Managed Process and level 3 Established Process, with a composition of 40% at level 3 and 60% at level 2. It can be concluded that most of the higher education institutions in Indonesia is not yet fully capable of implementing information security practices in accordance with international standards (ISO/IEC 27001:2013).
If seen from each clause or domain, the gap value between the current maturity level value and the expected level of maturity value varies for each clause (domain). The smallest gap (1 level) is in clause A5: Information Security Policy, clause A9: Access Control, and clause A11: Physical and environmental security. The biggest gap (4 levels) is in clause A14: System acquisition, development, and maintenance and clause A18: compliance.
Strict information security practices are very important for business organizations because they are the main key to ensuring the security of information assets owned by the organization. Controls on security practices are urgently needed to monitor, review and improve the security of organizational information. It is an ongoing process related to the development and implementation of security policies and procedures to determine who will do what, when and how, to prevent threats. Therefore, measurement of the level of maturity of information security practices can be done to see and analyse the gaps between real practices and expected ideal conditions.
For the development of ISMS research, an assessment can be conducted on more than 35 Universities or as many surveys as desired to Universities in Indonesia either by region or province or based on A or B accreditation degrees, it can also be based on these university categories such as University and Institute levels and even department levels .

Acknowledgement

We express our deep gratitude to the Indonesian Association of Higher Education in Informatics and Computing (APTIKOM) and the Center for Research and Community Development (P3M), Perbanas Institute in Jakarta, Indonesia and, R&D Asia e University, Kuala Lumpur, Malaysia. We also thanks to Prof. Dr., Richardus Eko Indrajit, Dr. Harya Damar Widiputra, Vice Rector, Academic and Information Technology Division and all research center staff for their help and support for this research. We also thank our colleagues who helped us make this research script better.

Bibliography

IGN Mantra, worked as a lecturer and researcher at Perbanas Institute for more than 20 years, teaching and researching, publications in the fields of computer and cyber security, security incident handling, digital forensics, networking and e-commerce. Previously worked at Security area for more than 20 years at ID-SIRTII (security incident response team), in collaboration with JP-CERT (Japan), MY-CERT (Malaysia), BSSN (National Cyber and Code), Indonesia DoD (Department of Defense), ICT Ministry, currently completing Ph.D research at Asia e University (Kuala Lumpur, Malaysia).

References

[1] Afrianto, Irawan, Taryana Suryana, dan Sufa'atin. 2015. Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI – SNI ISO/IEC 27001:2009 -Studi Kasus Perguruan Tinggi X. Bandung: Universitas Komputer Indonesia. https://doi.org/10.31937/si.v6i1.278.

[2] Badan Standardisasi Nasional. 2009. SNI ISO/IEC 27001:2009 Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan. Jakarta: Badan Standardisasi Nasional – BSN

[3] BSI UK (2014) 'Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013'. United Kingdom: BSI.

[4] Candiwan, M. Y. D., & Priyadi, Y. (2016). Analysis of Information Security Audit Using ISO 27001: 2013 & ISO 27002: 2013 at IT Division-X Company, In Bandung, Indonesia. *International Journal of Basic and Applied Science*, *4*(04), 77-88.

[5] ISACA. A Business Framework for the Governance and Management of Enterprise IT. United States of America: ISACA, 2012.

[6] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements. International organization for standardization

[7] Jennings, M. D. (2000). Gap analysis: Concepts, methods, and recent results. Landscape Ecology, 15(1), 5–20. https://doi.org/10.1023/A:1008184408300.

[8] Kurniawan, Endang & Riadi, Imam. Security Level Analysis of Academic Information Systems Based On Standard Iso 27002: 2013 Using SSE-CMM. International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 1, January 2018, 139-147

[9] Kusuma, R. A. (2014) Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001. Yogyakarta.

[10] Nasser, A. A. (2017). Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen. *Int. J. Sci. Res. in Multidisciplinary Studies Vol*, *3*, 11.

[11] Nurbojatmiko, A. Susanto and E. Shobariah, "Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO Depok City," 2016 4th International Conference on Cyber and IT Service Management, Bandung, 2016, pp. 1-6. https://doi.org/10.1109/CITSM.2016.7577471.

[12] Proença, D., & Borbinha, J. (2018, July). Information security management systems-a maturity model based on ISO/IEC 27001. In *International Conference on Business Information Systems* (pp. 102-114). Springer, Cham. https://doi.org/10.1007/978-3-319-93931-5_8.

[13] Rukh, L., & Malik, A. A. (2017, April). Swiss army knife of software processes generic framework of ISO 27001 and its mapping on resource management. In *2017 International Conference on Communication Technologies (ComTech)* (pp. 12-15). IEEE. https://doi.org/10.1109/COMTECH.2017.8065742.

[14] Silanegara, Indra & Bayu Adhi Tama. 2015. Strategi Pemilhan Kontraktor Perangkat Lunak Dengan Memanfaatkan Pengetahuan Terhadap Capability Maturity Model Integration for development (CMMI for Dev).

[15] Suwito M.H., Matsumoto S., Kawamoto J., Gollmann D., Sakurai K. (2016) An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, vol 376. Springer, Singapore. https://doi.org/10.1007/978-981-10-0557-2_69.