Journal of Theoretical and Applied Information Technology
28th February 2022. Vol.100. No 4
2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMPARATIVE STUDY OF INFORMATION SECURITY EVALUATION MODELS FOR INDONESIA GOVERNMENT

MUHAMMAD RADITYA PUTRA DEWANTO[1] , TANTY OKTAVIA[2], DAVID SUNDARAM[3]
[1,2]Information System Department School of Information Systems Bina Nusantara University, Jakarta, Indonesia 11480
[3]Department of Information Systems and Operations Management University of Auckland, Private Bag 92019, Auckland, 1142, New Zealand
E-mail: [1]muhammad.dewanto001@binus.ac.id, [2]toktavia@binus.edu, [3]d.sundaram@auckland.ac.nz

ABSTRACT

The stream in which every bit of information shared and viewed has been rapidly increasing at the current era, with speed like never unlike in previous generations. Because of that, there is dire need to effectively secure this information stream in order to prevent compromise from any risk and threats. This is particularly true for government sector that holds highly classified information crucial for the country operations. Indonesia government strive to protect and to better maintain information through an adoption of a robust security implementation within the many bodies of government throughout the country, however for an implementation to be robust the first time is near impossible. Robustness is achieved through rigor evaluation that actively assess the performance and effectiveness of that implementation to know its resiliency in withstanding attacks and efficient in its application. For this reason, KAMI Index is developed in order to evaluate and assess the maturity and the readiness of information security in each government agency, but does it reliable and accurate? To answer, this research will make a comparison to an existing evaluation frameworks or models proposed by other researchers that study the topic of information security with regards to different aspects that exists within it. By making a comparison, an analysis for an existing model what aspects that they do better or best compared to KAMI Index can be perform so that a suitable recommendation and suggestion can be made. This research will be conducted through Systematic Literature Review (SLR) methodology, this paper will also provide an explanation of alternatives information security evaluation models or frameworks, and the reason why these models can be used to improve or even replace the KAMI Index model. Results from this research includes an alternatives models to KAMI Index and identified IS aspects crucial for evaluation.

Keywords: *KAMI Index, Information Security, Information Security Evaluation, Government, Comparative Study*

1. INTRODUCTION

Information Security (IS) has seen a rapid development in the past few years, with every organizations in the world may it private or public has developed their own version of implementation in the form of Information Security Management System (ISMS) that is suited and customize to manage their information assets and resource effectively. There exist a several standards that serve as a guideline to this implementation such as the well-known international standards ISO 27001[1] and a nationally developed one such as NIST framework[2] that can be use by any organizations across the world that hopefully prevents or minimize the exposures of information asset from many risks and threats which then translates to maintainability and manageability of IS.

Indonesia, as one of the countries in the world that has taken a step forward toward improvement of E-government[3], is fully aware of the importance of IS especially within their government agencies that scattered across the many region of the country. For this reason, Indonesia has published several laws and guidelines that leads to establishment of cybersecurity field in many agencies which positively impact the assurance to information security[4], in addition to a published laws and guidelines, Indonesia government also developed KAMI Index, it is an evaluation model used to evaluate the maturity of security measures in each government agency in Indonesia[5] and mainly to rate their ”readiness and preparedness”, based on the

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

officials says[6]. Even if an organization thinks that their ISMS is properly implemented, there may exist other unaccounted factors why they are still prone to danger to information risk and threats[7]

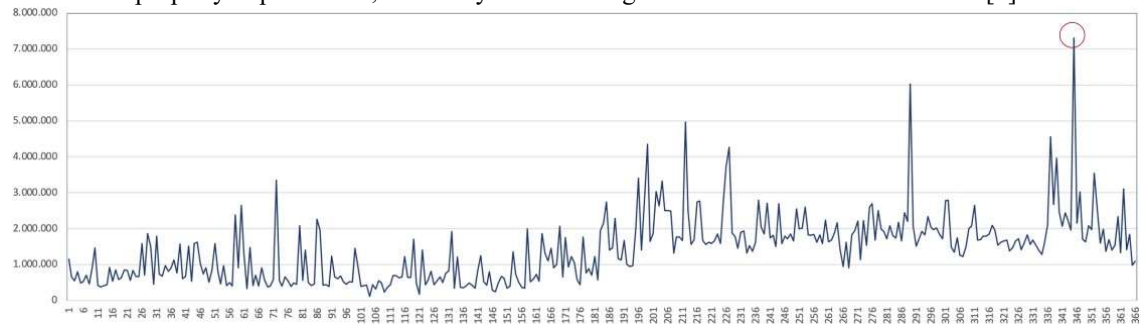

Figure 1: Cyber Traffic anomaly in 2020 (Courtesy of Report published by BSSN

which the organization is unaware of, this can lead to a data breach, cyberattack, information theft, and other related incidents that can catch them off-guard and cause havoc for internal operations. Therefore, there need for an evaluation model and KAMI Index will serve just that for Indonesia government.

However, even with the implementation of ISMS in place within many government agencies and the existence of KAMI Index to evaluate them. Rising tides of cyber-related incidents keep surging with alarming rate within Indonesia, it is quite questionable whether government's agencies able to withstand these attacks. In a report from State Cyber and Crypto Agency (BSSN), last year in 2020 when the pandemic recently hits the country, BSSN has detected approximately 495 million case of cyberattack in the range from 1st of January to December 31st[8]. This number is four times higher than in 2019 which approximate to only 39 million according to a trusted news article[9]. This does disturb the operations of many organizations in Indonesia especially government agencies in many regions in the country. While there are no explicit numbers of how many agencies affected by cyberattack within the report, only a number that totals of 1293 complaint from organizations in different sectors with 660 comes from the government.

With that said, the purpose of conducting this research is to study of other models out there that is better if not similar to KAMI Index evaluation model. Comparison between these models with KAMI Index will be made. Through it, this paper will provide some analysis, insight, thoughts, reason, and explanation why other models are superior to KAMI Index or vice-versa by pointing out the different aspects of what makes that model possible, and also points out each of its strongest points.

Contribution of the research through this paper is mainly knowledge, because this paper will provide an information regarding the different aspects that serve as the foundation to IS implementation in organization that sometimes overlook which can hinder the full potentials to IS implementation, especially within government sector. This paper will also provide a brief overview regarding the condition of IS and cybersecurity in Indonesia while keeping in mind that government digitalization movement has been prominent within the country. Aside from these, other contributions from this paper is in a form of comparison and evaluation for KAMI Index model, so that we can find other better alternatives to evaluate the security aspect within Indonesia government.

While the main highlight of this study is Indonesia government and it IS evaluation model (KAMI Index). Results and informational findings of this study is not exclusively unique to the context of this one country only, this is because while Information security implementation in many organization and countries are quite different between each other. The fundamental science of this topic is the same. All the researchers that research this topic, study upon the same IS aspects that are discussed in this paper. Furthermore, suggested IS evaluation models which are provided in this paper does not cater to the characteristics of one organization or government only, in fact, since all the models provided in this paper are proposed by variety researchers in many different countries, application of it is universal. For the context of Indonesia. Uniqueness of the findings in this paper is that it serves as a suggestion to improve KAMI Index, although implicitly, this is because based on analysis KAMI Index mainly focusing in only one aspect of IS, instead of all aspect resulting in its process quite ineffective as an evaluation model.

For the execution, this research is conducted fully online with the use of WFH (Work from home) ethic due to covid-19 still active in the country making data gathering on-site difficult to do. The methodology used will be Systematic Literature Review (SLR), which is finding and gathering data through reviewing different study materials

(literatures) that is relevant to the topic such as paper or articles written by other researchers tackling this domain. Systematic in SLR means that a proper process is conducted for selecting the materials for study in order to find the most relevant and information-rich references that can serve as the foundation for this paper, this is also to ensure that suggestion and recommendations provided in this paper based on facts and evidences that supports it. For this reason, to ensure a proper execution of SLR methodology used in this study, a protocol will be defined and followed. This selected protocol will be based on Chitu Okoli and Kira Schrabram[10] which will be further explained in section 3.

2. LITERATURE REVIEW

This section will provide the definition of terms used for this research based on various studies that have been collected.

2.1 Information Security

Information Security or IS for short, according to research conducted by Gaston Concha and Paula Suarez[11]. Refers to preventive or reactive mechanisms or protocol used to protect any information within private or public sector organization. There are three principles that serves as the baseline for IS implementation, principles such as: Confidentiality, Integrity and Availability. Otherwise known as the CIA Triad[12]. functions as a goal for any implementations of security in every organization, especially true for government sector, even though E-Government movement encourage for open information to the public, there are some limitations to it since but there are also exception such as internal information that is crucial to the lifeline of the government organization and even to the lifeline of the country itself.

Information Security touched on various aspects that is present within organizations, one of which includes the working staff as one of the crucial factors for security and one of the most relevant subject in many research papers that study IS topic, mainly their behavior towards IS policy compliance[13] and their participation in securing information asset within the organization. While it is true that IS often only touch on the technical side of things, the social domain is equally important to its performance. The effectiveness of IS implementation within organization can only be called successful if the social and technical of it goes hand-in-hand together and formed a culture.

2.2 Information Security Management System

Each countries have their own secrets that cannot be shared with others, hence there are exist a management system that serve as a comprehensive set of policies for organization to manage the risk of information asset, such management system are called ISMS or Information Security Management System[14]. This is the form of IS implementation within many organizations including the government sectors. M. Khyavi and M. Rahimi define ISMS[15] in their paper as a special standard method that considers all aspect within security with management view and based on the approved standards by ISO that distinguish the correct and proper way to design, implement, running, and managing that security. Furthermore, mentioned in the paper quoted, ”In this system all assets (tangible and intangible), vulnerabilities, risks, threats and controls would be considered and based on that a new security comprehensive scheme would be presented.”

2.3 Information Security Evaluation

Information Security Evaluation is a process to assess or evaluate the security implementation that protects an informational asset in organization by determining the level of its security risk and determine that risk priority based on impact and cost to the asset[16]. The main purpose in conducting this evaluation is quite explanatory to its name. It is to evaluate IS implementation within organization that implemented it. The main process of evaluation includes identify and asses risk present within the system[17], measure the preparedness of the security based on the present technology[18][6], Test the effectiveness of IS implementation based on real-world scenario[19], plan for improvement[20], Etc.

2.4 Information Security Maturity

Much of the research papers conducted for this topic refer Information Security Maturity as a model. In one of the researches conducted by E. Rigon et al. in his paper a maturity model ”provides a guide for a full security program. It also defines the order in which security elements must be implemented, encourages the use of standards of best practices and provides a means to compare security programs”[21]. In addition A.Rabii et al[22] explained IS maturity in their paper, in which it serve as tools for evaluation to assess the possibility of improvement for a specific organization. Furthermore, main functions of maturity are means for assessing and benchmarking the performance of security implementation, roadmap for improvement on

existing model, means to identify gaps, and lastly to develop an improvement plan.
However, other research albeit quiet differently though implicitly define maturity as a set of metrics to rate the area of focus of IS implementation like from the research conducted by F.Alqahtani[23].

2.5 KAMI Index

According to article from National Cyber and Crypto Agency (Badan Siber dan Sandi Negara)[6]. KAMI Index is an application which is used as a tool to assess and evaluate the level of readiness (Completeness and Maturity) of the application of information security based on the criteria of SNI ISO/IEC 27001, namely Governance, Risk Management, Framework, Asset Management, Technological Aspects with a supplement of Safeguarding the Engagement of Third Party Providers Services, Cloud Infrastructure Services Security and Personal Data Protection. However, further in the articles, it also explains that KAMI only used to provide an overview of the state of readiness of the already implemented framework for infosec, and not intended to analyze feasibility or effectiveness of the security. Furthermore, KAMI Index is a form of Information Security governance/management system implementation policy for electronic-based public service provider for good IT governance, for this reason, KAMI Index defines 11 control area for IS which is based on ISO 27001, which includes:

1. Information security policy
2. Information security organization
3. Asset management
4. Human resource related to Information Security
5. Physical environment security
6. Operational communication and management
7. Access control
8. Procurement/acquisition, development and information system maintenance
9. Information security incident management
10. business continuity management
11. Obedience.

These 11-control areas are shortened into 6 area that KAMI index evaluates within agencies; the 6 scopes include:

1 **Information security governance:** Evaluates the overall readiness of security governance functions, task, and duties performed by information security managers within the agencies

2 **Information security risk management:** Evaluates the readiness risk assessment procedures as the basis information security management.

3 **Information security framework:** Evaluates the readiness of framework which includes the implemented policies and procedures regarding information security management.

4 **Information asset management:** Evaluates the security completeness of information asset usage cycle.

5 **Information security technology:** Evaluate the completeness, consistency and the effectiveness of technology usage within the agency.

6 **The role of Information and Communication Technology (ICT):** Evaluates the dependency of ICT services to run the agency's operations and task.

2.6 ISO 27001

ISO 27001 is an internationally agreed standard for Information security management system in many organizations in various sector in the world. This standard provides guidelines for organizations to manage their information security and address risk that can bring benefit to not only the organizations themselves, but also to their stakeholders[24]. KAMI Index evaluation model is built based on the localized version of this standard called SNI/ISO 27001[6] which is very much the same with the original version and very much touched on the same control area.

However according to one study[25], the controls that ISO 27001 provided doesn't necessarily conform to organizations with low adoption of IT and automation within their system which leads to a higher cost due to the possibility of only partial automation through hardware and software tools which makes its implementation ineffective, furthermore this paper addressed another problem to this standard, such is the lack of adequate

guidance on cultural and psychological dimensions that is relevant to ensure employees compliance towards IS policy within the organization. That said though. while note entirely perfect, ISO 27001 still provide a full and comprehensive metrics that can be use by organizations to develop their own customize version of IS model for analysis of the risk[26], management of risk[16], or IS governance model[27].

3. RESEARCH METHOD

The method this research will be using is SLR which is a short for Systematic Literature Review. This method focuses on processing journals, articles or other study materials to find the information needed to for the topics at hand. The reason for choosing SLR as the main method for the research is because of the ongoing covid-19 pandemic in Indonesia, especially in the current lockdown situation that still active where we can't travel freely due to many roads are closed to limit mobility. In SLR methodology, the study materials will be sought from various well-known publishers such as ACM, IEEE, Science Direct, Wiley, and Emerald. Additional materials found in exploratory study that is reliable, suitable and within categories defined for this methodology is also included. For the information or data attached to this research paper to be concrete, as well as relevant, rigorous procedure or protocol is conducted. The protocol to be use in this SLR methodology is based on the suggestion by Chitu Okoli and Kira Schrabram in their research article[10]. This protocol is tailored based on the research need and the current situation while still keeping the rigorousness of the process so that information extracted from all the materials remain credible, accurate, and valid which guarantee the authenticity of this paper. The protocol itself is designed and focused for Information System researcher that conduct their research mainly through SLR methodology. This protocol ensures the validity and reliability of information extracted from many different sources by going through a 4-phase process as explained in the *Figure 2*. this process helps in maximizing the output of the research with the goals of making a systematic, explicit, comprehensive, and reproducible research which automatically defines its quality as one of the study material that can help other researchers and as a scientific knowledge for the related topic.

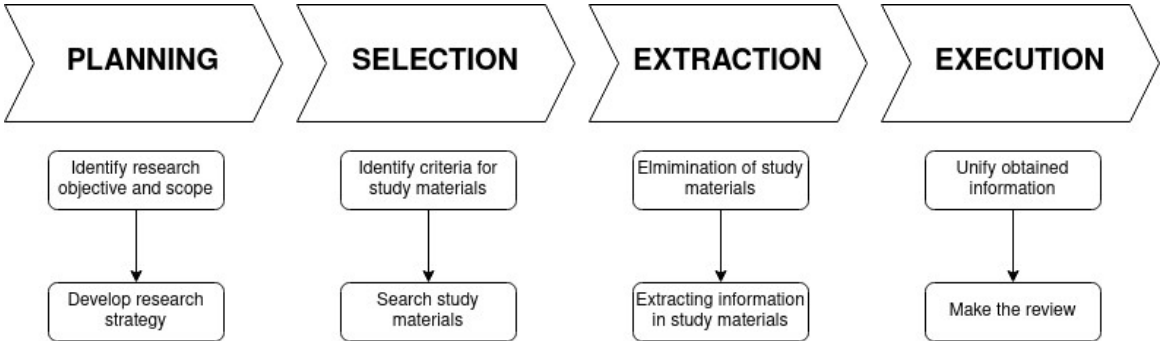

Figure 2: SLR Process based on Chitu Okoli and Kira Schrabram

3.1 Planning

Planning is the first phase in the research method. In this phase defined the objectives of the research, and the formulation of the research questions.

3.1.1 Research objectives

The objectives in conducting this research is to:

- Study other evaluation models similar to KAMI Index
- Compare other evaluation models to KAMI Index
- Suggest a viable alternative for evaluation model based on the comparison
- Recommends an improvement for KAMI Index

3.1.2 Research questions

Formulated questions that is asked for this research are:

- What are aspects that needs to be evaluated in IS?
- What other models that can be used to replace KAMI Index?

3.1.3 Research strategy

In addition to the already mentioned research process. The flow of the research is like this:

- **Step 1:** Define the purpose and objectives of the research.
- **Step 2:** Form the research questions.
- **Step 3:** Create the protocol to be use for the research based on the chosen research method.
- **Step 4:** Search the literature in journals or publishers. this will later serve as the main knowledge foundation for the research.
- **Step 5:** Filter the literature by reading through its abstracts if it suitable for the study. Literature selected in this step becomes the ”Candidate studies”
- **Step 6:** Define the criteria for ”Selected studies”
- **Step 7:** Read the literature for the points that it’s trying to convey, and check if its fit for ”Selected studies”.
- **Step 8:** Create a brief summary of literature in ”Selected studies” to aid in recall .
- **Step 9:** Write the research paper.

3.2 Selection

Selection phase is conducted in order to select study materials that is suitable for the research. Procedures in this phase includes defining the criteria for materials selection, choosing the sources to search the materials, lastly is search strategy in which string used for searching is defined here.

3.2.1 Study materials criteria

For this research, the criteria used to search a literature are related to Information Security research topic in general such as: ”Policy”, ”Risk Management”, ”Framework” or ”model”, and ”Evaluation”. Additional criteria include ”Government” and ”Organization” since the scope of this study is mainly IS within government sector, and that sector is fundamentally an organization.

3.2.2 Material sources

The main sources of the literature come from journals and publishers of research papers. There are 5 that has been chosen to search the literature from, which are: ACM, IEEE, Science Direct, Emerald, and Wiley. Aside from these 5 sources. There are a few study materials that comes from other sources that is not publishers or journals which are news articles and official government’s website that is legitimate and reliable in delivering a fact. However, this additional source only serves as a side reference that complements the main one.

3.2.3 Search strategy

The search for the materials is conducted using the same search string that is constructed based on the defined criteria, which is: **”Information Security” AND Government AND Framework AND Model AND Policy AND Management AND organization AND Evaluation**.

Other aspect related to search such as range of years are set from 2011-2021 or 10 years prior, this is so we can find the most relevant materials as possible.

3.3 Extraction

This section will provide an explanation and an overview of the process conducted in order to extract the most suitable materials that will serve as the main reference for the research. These main references will be used to find the answers of the research questions.

3.3.1 Selection process

In the selection process, all the materials pass through different three-steps process as seen in *Table 1*. For context, ”Studies Found” refers to the number results of materials found within journals or publishers’ database after doing the search with use of the search string. ”Candidate Studies” refers to the saved materials that is found in the ”Studies Found” due to the abstract is align with the theme of the research. ”Selected studies” is the permanently selected materials that has been given a full read of its content and found that it contains the required knowledge, model, framework, theory, or insight that is suitable to the research. Aside from this aspects, other criteria that is defined as a checklist in order to search for ”Selected studies” are:

- Provide an applicable model, framework, tools or working theory of an infosec evaluation.
- Contain three or more keywords defined for the research

- Provide a case study that can be used for an example
- good amount and reliable data backing the study
- Simple on explanation but deep on insight

Table 1: Filtering Process of materials

Source	Studies Found	Candidate Studies	Selected Studies
ACM	366	65	21
IEEE	1	0	0
Science Direct	559	48	21
Wiley	335	11	6
Emerald	667	22	15
Total	**1928**	**146**	**63**

4. RESULTS AND FINDINGS

After going through the Systematic Literature Review (SLR) process via the protocol defined for this research that is explained previously. This section will provide an analysis of all the data and information that has been gathered and compiled for this study. The analysis will analyze a relevant information such as year and country of origins of all the studies. This sections also provide the findings that answers the research questions defined in the previous sections.

4.1 Studies Analysis

For the sake of transparency this section analyzes the total of published studies within a certain year and the country which it originates.

4.1.1 Year of studies

Frequency of the paper that has been search within the range of year from 2011 to 2021 can be seen in *Table **2***. Much of the papers conducted for IS topic published within the year of 2020 making the most productive year conducted for the research. This is due to the widespread of global pandemic of covid-19 with many countries in the world limiting outside activities for their citizens, this results in high frequencies of cyber related incident that occur within the period of the year. Aside from the year 2020. high number of papers also found within the year 2012, 2014, and 2018 each with 7 papers found.

Table 2: Number of studies based on year

Year	# Published papers	% Published papers
2011	5	7.94%
2012	7	11.11%
2013	3	4.76%
2014	7	11.11%
2015	6	9.52%
2016	3	4.76%
2017	6	9.52%
2018	7	11.11%
2019	5	7.94%
2020	10	15.87%
2021	4	6.35%
Total	63	

4.1.2 Country of Origins

While various selected studies that has been found for this research comes from a few different publishers. These materials originated from various countries in the world, which can be seen in *Table **3***. Based on the table, majority of institution that conducted the IS research has been originated in the country of USA, with the total number of 36 authors from 22 different institution has written the research paper for this topic, main reason why there are many security researchers originates from USA mainly because this country becomes the forefront in the field of cyber security due to their high advancement of technological level compare to the other country, and pretty much of the known company such as: Google, Apple, Microsoft, Etc. are located within the country, making it the highest priority in order to properly and effectively secure any informational asset since cyber incidents are also more pronounce there. Other countries besides USA that has many researchers study IS topic are Greece, Sweden, Italy, UK, and Germany. One reason why majority of the research originates from these countries is because many of the IS standards like ISO 2700-series for example comes from Europe, making these countries more advanced in term of their IS implementation.

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

4.2 Different Aspects of IS

Based on what have been gathered according to the collection of the study materials. There are mainly three aspects that made up IS implementation within an organization. These aspects are important in which an effective and efficient information security management system that is perfectly serve its role and does not burden its operational.

4.2.1 Social

Social aspects of Information Security, as the name implies the considerations of IS implementations based on organization's environment and cultures. This aspect mainly covers how human actors–specifically staff–fulfill their role of security within organization, their behavior towards security policy compliance, and also to covers how organizations properly manage this aspect in order to prevent any risk that can threaten their informational assets. There are few studies that have collected that mainly focused on this aspect, each of the studies stressed how equally importance this aspect with the other two aspects. Like explained in one of the paper that study the importance of this social aspect[28], it mentioned how information security effort within the organization can be bogged down due to the staff not fully or entirely comply with the defined policy that is active which is the behavioral problem towards the security, and the main factor of that problem is the policy itself that is rigid and can hinder the staff's work, this effectively create a cycle of problems for the organization as it needs a policies to maintain the information security but to do that it needs a compliance from the staff which themselves tends to avoid due to it hinders their job.

Human factors in the context of security, are known as the weakest link in the chain, meaning they are the most valuable targets for hackers or other malicious actors to compromise the organization's IS. This is mainly proven by staff or other employees that tends to avoid compliance of security policies, because of this trait they are categorize as "Insiders Threat". This term refers to insiders that is authorized to access the organization's internal system but has a malicious purpose that pose a threat to the operations which in this case, becomes the risk to information security. The motives of insiders threat are varied[29], but speaking in the context of social aspects of IS, it is the same reason why employee avoid compliance to the policies.

This bad behavior of security policies avoidance are the main challenge for organizations to improve their own security posture, one of the solution is through consistent security practices from top management to training program to policy[30] that strive to foster a kind of unity through shared perception of what is called information security climate or ISC according to the study which able to eliminate the problem of security avoidance intention by quote: "giving a clear ground on which employees determine their agreement and conformity with values that the security policies could bring once followed", or in other words the understanding of the importance of security implementations in the organization.

Aside from security practices to training program. Other solution to social aspect problem is to improve relation. Research by M. Khyavi et al[15], study the importance of relation between high and lower management within organization, in which good relation can lead to trust and better cooperation through flexibility and interconnection between different management levels that leads to betterment of IS performance within organization. Problems such as avoidance to security policies that is mentioned previously can be negate because thanks to the improvement of relations, communication from top-to-bottom are also improve, which means a clear understanding of security goals, roles, and decision, leads to clear employees responsibilities, commitments for themselves and for their firms (they know themselves effective in their organization) and etc.

One question remains, what is this social aspect implications towards IS evaluation model that is the main highlight of this research? As an emphasis, based on the explanation on the previous paragraph, there are three factors that lay the foundation of social aspects that builds IS. Those are security policy, employee's behavior towards security policy, and relations between management. These three factors can be translated as just Policy, consistent security practice or training program, and flexibility of communication respectively, which can be measure and effectively evaluate within an evaluation model. In short, this social aspect can serve as one of the parts that needs to be evaluated in order to improve security performance within an organization, or in the context of this research, government agency.

Table 4 Shows the different studies that have a focus in this aspect. Many of the points that has been stated in this section found within each of the studies. Practical implications from these studies includes collaboration between manager and staff, evaluation model that measures the performance of IS based on how well the flexibility of communication between the higher level and the lower level, and also the insight that these materials provide regarding behavior of different actors within the organization regarding IS policy and other implemented regulations.

4.2.2 Technical

Technical aspect of information security refers to technological implementations with the purpose to improve the organization security performance which leads to the improvement information security assurance. This aspect serves as a solution in securing information asset within the organization, protecting the confidentiality, integrity and the authenticity of said information. An example of the technology that is usually adopted and integrated are Firewalls, Antivirus software, Intrusion Detection System, Access controls, Password manager, and other similar tools. In some study, technological factors such as the adoption of many security tools within organization showed the maturity of organization infrastructure which strongly increases its readiness in combating cyber-attacks[31]. Furthermore, it brings a positive performance impact in performing a security task.

However, many implementation technologies do not mean that it is effective in securing the infrastructure, at least not yet, not until the IT security staff (ITsec) has undergo a proper training to secure the organization's network through the utilization of the adopted technologies. Professional and experienced ITsec staff can bring out the full performance of adopted technologies making their task done much more effectively and efficiently, especially when handling cyber risks that poses a threat to organization's network. Hence, this is why that it is paramount to conduct an assessment to measure their capabilities in order to know what are that they lacking and relates that to network/physical security domain within organization that requires attention which later on, a training program can be propose in order for ITsec to properly secure that domain[32].

While improvement of ITsec staff can lead to an effective securing of organization's infrastructure from cyber-attacks. Proper maintenance of all the used technologies also need to be conducted. This is so that security vulnerabilities do not plague the system and becomes a threat later. What it means by vulnerabilities is a security loopholes that is present within many software of tools that is presence in the system, this loopholes can be exploited by attackers to gain access to organization's infrastructure effectively compromising information security[2] leading to a cyber incident known as data breach. One of the results of such incident is the negative impact of stakeholder's trust. A study explained quote: "In the aftermath of a breach, firms are challenged to mitigate the long-term financial impact by restoring customer trust. These reports indicate that vulnerabilities pose permanent risks for firms for which they need to be prepared." Further into the study, the risks of this breach is diverse with it such as: "loss or theft of personal data, loss or theft of commercially sensitive information, inoperable IT systems (making the business unable to function after being hacked), intellectual property infringement, and extortion, which can lead to serious financial damage"[33].

Same as social aspect in previous section, technological aspect also contributes in providing additional factors that needs to be checked for evaluation model in order to be complete in evaluating IS in government agency so to better provide an overview regarding their security environment and to highlight the area of security that can be improve. The additional factor derived from this aspect are: Implemented technologies within organization and its usage, ITsec professionals' overall capabilities, and lastly is the version of the software and tools.

Table 5 shows the studies that provide a context and an explanation regarding the technical aspect of IS. While only a few, these studies provide the needed context and insight regarding the place and the role of this aspect within ISMS. Practical implications that can be defined based on the findings from this studies: technology is important and serves as the foundation in which a proper ISMS can be built, and while that is mainly the case in many of the organizations, proper maintenance, usage, reason for its adoption, or development can serve a long way for organization survival both in securing their own infrastructure from threats and risk through the use of this technology and also in

managing their own resource since adopting these technologies can be expensive.

4.2.3 Management

Management aspect which defined as Information Security Management or ISM according to many studies that focus on this aspect [34][35][7]. ISM within organization considers all the factors defined for both technical and social aspect for a proper decision making regarding security within the organization, in addition organizational factors such as its economics, asset and resource, organization's goals, and also the risks to information is also included within ISM making it the culmination of many aspect of IS implementation within organization. If that is the case, so what is the task of ISM? ISM handles task such as: risk assessment, implementation of policies, controls and regulation, promote awareness, and lastly to monitor and evaluate[28]. To elaborate risk assessment task is to provide a decision maker an information regarding the risk factor that affect the operational. Policies, controls and other regulations are used to decrease the identified risk to an acceptable level. Promote awareness through training to further decrease the likelihood of risk by a person. lastly in order to evaluate and measure potential level of risk factors and exposure a monitor and evaluation process is needed.

While managing IS from threats is the main purpose to ISM, however the overall threat landscape in this day and age is very dynamic that a full maturity in only one aspect of IS does not translate to the overall readiness of the organization's system when dealing with cyber-attacks or other cyber risk that may poses a threat, that's why an extra attention to other aspect is also becomes a priority in order for IS implementation within organization to be effective. While this is true, some studies also mentioned that perfect implementation in cyber security to is impossible to do, this is due to the fact that it is always keep on changing according to advancement of technology and does not stay in one place[36], which also true to the number of threats that is always keeps on rising accordingly. Therefore a "good enough" mindset implementation that has considered all the technical, social and the rest of the management aspect is a best course of action in overall IS.

Further elaborate of the word "good enough". Study conducted by E. Bergstrom et al. [36] explained about this word in detail. The full term of it is according to the study; "Knowing how to be 'good enough'", with the context is for organization to perceive and understand that security landscape in cyber landscape is always changing, also there are no fixed recipe when it comes to the best implementation or practice regarding this landscape. So, adoption of this 'good enough' mindset ensure the security process to be refined and adapted to change. Further into the study, this term does not come alone, it is accompanied by 3 more "Knowing to..." that has been formulated in the study as a solution for the dynamic condition of cyber security. According to the study this other "knowing to..." are:

- **Knowing to hurry slowly:** Take it slow but consistent progress
- **Knowing there is no silver bullet:** Software is just a tool, not a solution.
- **Knowing the bigger picture:** realize the process as a one joint effort between many aspects.

Defined mindset above and developing it naturally within organization to ease the tension to security implementation is the best act psychologically. Economically, managers also need to keep an eye out of the investment for all the implementation within the organization. However, instead of investment, some study instead define this as a measure that estimate the success value in achieving the level of security that is originally planned[28], not quite as a target instead act as one of the security metric that not only to measure the success, but to also rate the performance if it good enough to achieve the organization end goal in ISM.

To complete. An effective ISM always refers to an existing standard that serve as a best practice and are used to implement the ISM system or ISMS. This security standards such as ISO/IEC2700 series, COBIT framework, NIST SP800-series, and ISF best practice exist to address the most problems usually encountered in information security and give an overview regarding its mitigation[30]. However, while these standards are agreed internationally and are implemented worldwide, does not mean that its free from problem and that organizations can be freely use it. Instead, it has several problems making it difficult to properly implement this standards within organization, further into the study from R. Diesch et al. explained about problems, one of which is that these standards is misleading risk mitigation strategies due to the lack of concrete countermeasures and the step-by-step of action plan that should be define for this. These standards only provide the "why" of the implementation and not the "how".

Back in the context of an evaluation model. Measurement factor that can be used as an evaluation points in management aspects are actually the same that is defined for technical and social aspect in

previous subsections, but with addition such as: Investment of security implementation, Adaptability of ISMS, and adherence to standard.

Table ***6*** provides the different studies in which information of management aspect in IS can be found and extracted. These studies contains some insight and thoughts regarding management aspect in general within the context of Information security, which pretty much informed about the many challenges that must be faced by decision makers in order to make a correct judgement regarding to managing IS within the organization, since every decision is crucial. This further imply that one bad decision can prove fatal and can have a lasting impact in operations, in order to prevent this an informed knowledge of the vulnerabilities and risk in both aspects of IS (Social and Technical), organization's goals and targets, organization's scale, and also the information regarding the resources that the organization has are needed to be satisfied in order set a correct course actions in order to effectively managing IS within the organization. Since every organizations are constraint with resources wise management decision can bring a difference.

4.3 Comparison of IS Evaluation Models

Explained in section 2 about KAMI Index. There are 6 areas that is evaluated within government agencies that includes all the aspect of IS which are: Technical, Social, and Management. In other words, KAMI Index already evaluates the different aspect of IS that is present in many government agencies in Indonesia, however. While this evaluation model is used to evaluate the maturity and readiness of IS aspects, it is not intended to analyze the appropriateness and the effectiveness of measures that are already present within the agencies system as it is only gives a basic overview of the readiness condition of IS framework within agency. This is the main problem of KAMI Index as it does not give any improvement plan, guidance, or recommendations in order reduce possible security threats within the system and also to reach the mature stage possible that may benefit the agencies, which is quite contrary to the purpose of IS evaluation model in general that exist and conducted within many organizations for this purpose.

Based on this evaluation, KAMI Index evaluation model is not enough to evaluate IS maturity in many government agencies in Indonesia as it only gives a basic overview and not thoroughly map the IS evaluation to its mature stage. Therefore, alternatives to this evaluation model is needed in order to not only gives an overview but also to help in improving and perfecting the existing implementation within government agencies.

PRISM evaluation model by R. Goel Et al[17], the first model recommended as an alternative to KAMI Index. PRISM can be used to evaluate the risk management and also the areas or vectors within the agency cybersecurity using quantitative value, while this can serve as a way to draw an overview and inspect the maturity to the agencies IS implementation, main purpose of this process is to identify possible risk an threats that may pose a problem, which later identify the approach to resolve that problem. Main benefit of this model is its flexibility of adoption and its ability to provide evaluation within the context of the agency resource constraint, making it an attractive alternative to KAMI Index due to its high adaptability to many government agencies system.

E. Rigon Et al.[21]. Proposed a method for ISM through periodical evaluation of security maturity and continuous improvement of its control. Standard that this proposed model based on is quite varied which consist of: ISO 27001 that served as its structure which allows "continuous evaluation and improvement", ISO 27002 that defined its control area, ISO 27005 provide support for the improvement actions that is based on risk, lastly this model also draw some influence from COBIT which serve as its base measurement for the maturity assessment. The variety of standards present in this model makes the evaluation process completer and more effective since it also provides the action plan needed for improvement. Furthermore, it also provides ways for continuous monitoring of the action plan to evaluate possible problems in its execution within an agency. Compared to KAMI Index, this evaluation model by E. Rigon Et al is like an upgrade.

These two models above are the recommended models that can be used by Indonesia government to evaluate the IS implementation within agencies. While it is recommended due to the similarity with KAMI Index, the recommended models may serves as an upgrade because of the completeness of its process by not only gives an overview regarding the condition of the security implementation but also providing an improvement plan for the agencies evaluated by these models. While this research found various evaluation models in many different materials, PRISM and E. Rigon Et al model are the ones that come close to KAMI Index evaluation model because of the same adopted standards, evaluation of IS maturity, and with regards to social, technical and the management aspect of IS.

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

5. DISCUSSION

In the finding section of this paper, there are two recommended models that can serve as an alternative evaluation model for KAMI Index. These models can be use by the government to evaluate the IS maturity of various agencies in many regions of Indonesia due to their flexibility and adaptability that caters to each agencies technological and economic situation in the context of IS. While the main process of this models is evaluating the condition of IS maturity based on the defined international standards such as ISO 27001, which is the same process and standard that has been conducted with KAMI Index. However, unlike KAMI Index that only gives a basic overview regarding the condition of IS implementation within the system, the recommended models taking the step forward by providing a plan for improvement needed based on the evaluation result. Furthermore, continuous monitoring is also conducted to detect any other problem that lies within the improved framework in agencies IS.

Theoretically speaking, the implementation of one of the recommended models may sound good on paper because of the improvement that these models can give when compare to the old ones that is KAMI Index. Practically it can be different though, because not all the agencies adopt a modern or technological approach to there is which is the prerequisite of IS evaluation models. While it is true that to better evaluate a security related to information, other aspects such as management and social that does not or only relate a little to technology becomes the highest priority based on many studies that technology within the technical aspect is only a tools or a means to an end, with that end is to protect information asset. However, the main object of evaluation to these evaluation models is the technological system process in which IS can be secured, if this is absent within the agencies and only a traditional process is present, this can hinder the evaluation process. Not only that, an optimized improvement may still lead to a higher cost even if it already caters to the agencies monetary. This paper was not to conduct a deeper studies regarding the different technological condition in various government agencies, however, in one material[5] it mentioned that there are inequalities regarding ICT adoption in various agencies, this points out that in some degree recommended evaluation models can be used to evaluate IS implementation for agencies that still have traditional non-technological method, different evaluation approach for this approach are needed.

6. CONCLUSION

This study has been conducted with the purpose to find out other alternatives to information security evaluation models that can serve as an improvement to KAMI Index, a model created by Indonesia government that has a purpose to evaluate the maturity of various government agencies IS implementation within the country. Main reason why there is need to search for an alternative model to KAMI Index is because, KAMI Index only provide the evaluated agency a basic overview regarding their IS maturity condition and does not provide any assessment regarding their effectiveness and appropriateness when dealing with incident. KAMI Index also does not provide any sort of plan for improvement that can serve as a guideline or recommendation on how to properly secure, maintain, manage or implement their ISMS. This is a problem due to the recent frequency of cyberattack in Indonesia which makes information protection through ISMS even more important. While there are no fixed set of rules or guidelines for the implementation in various agencies, there need to be an evaluation to measure their reliability and to provide some sort of improvement. Which is what KAMI Index evaluation model lacks, and this paper provided a recommendation regarding a suitable evaluation model that is similar but also improve upon it.

Contribution to knowledge that is defined in section 1 of this paper has been achieved with identification of different aspects that exist within the Information security topic. In addition, through a comparative study of different IS evaluation models that has been conducted, alternatives for KAMI Index also has been provided. These results are achieved after going through a protocol model defined for Systematic Literature Review (SLR) research methodology. Additionally, with these results, implication for IT research contribution is it contributes a certain knowledge in the form of theory and a literature review that can be refer to by other researcher conducting an IT study that touches upon Information Security domain.

Uniqueness of this study regarding Indonesia, is that this study serves as a critics and correction for the adoption of KAMI Index as an evaluation model for IS in various agencies in Indonesia. As stated in previous sections. KAMI Index model is not enough or ineffective because it missed the point of what IS evaluation model supposed to do, which is supposed to actively assess the performance and effectiveness of organization's ISMS to know its resiliency in

withstanding attacks and efficient in its application and also to provide an actual improvements[37][21] [5].

Recommendations provided in this paper consist of two IS evaluation models that serves as an alternative to KAMI Index. First is PRISM evaluation model proposed by E.Goel et al[17] which evaluates and gives an overview regarding the condition of ISMS within agencies much like KAMI Index. However, the main purpose of this model is to identify various risk and threats present within the system with regards to different aspects of IS. Later, data of this identification process can be used to propose a suitable approach to deal with the problem. Benefit of this PRISM model is its high adaptability in its evaluation process within various agencies and cater to their resource constraint. The drawback is that unlike KAMI Index that mainly evaluates the maturity of agency's ISMS, this process only serve as a side task in PRISM and while it also gives a basic overview regarding its condition in the agencies, main priority of PRISM model is risk assessment. Other drawback is poor performance for evaluating agencies with little to no adoption of technology or agencies with traditional approach or pen-and-paper.

Second alternative model, is E. Rigon et al[21] proposed model. This evaluation model developed based on variety of international Information security standards that also includes ISO 27001, same standard adopted in KAMI Index. Compared to PRISM evaluation model, the evaluation process of this model very much identical to KAMI Index which is to evaluate IS maturity within the agencies, with addition to also provide an improvement plan and continuous monitoring that is needed for a proper IS implementation in various aspect within the agency. Main drawback of this model is quite the same as PRISM model, that is the difficulty in evaluating agencies with pen-and-paper approach to IS, while this model does not dependent on technology, assessing an agency that still has this approach is quite bothersome not just for this evaluation model, but any models in general.

7. LIMITATION AND SUGGESTION FOR FUTURE STUDY

In conducting this study, there are some limitation present that hinders the full potential of the study, which makes the information contained within this paper a bit limited and did not provide the wider context regarding information security in Indonesia government. The limitation of this study includes time constraint, limitation of information and reference that provide the wider scope regarding IS condition in Indonesia government. This limitation also includes the current condition of covid-19 pandemic that is still active in the country which limits travel due to the lockdown that still in place. All of this resulting in this paper only provide much smaller scale serves as a brief overview regarding the condition of IS in Indonesia government based on the evaluation model used to assessed these IS and not an in-depth study of this condition.

Suggestions for future study according to these limitations is an in-depth evaluation of how KAMI Index really works in the real-life scenario while also providing an in-depth research of how the condition of IS in the country of Indonesia. Since this research only serve as a brief introduction to what KAMI Index really is and what its main problems are based on other materials that study this model. So, an evaluation study through an interview with the one that proposed this model, or by spreading questionnaire to an agency that evaluated by this model to know their thoughts about KAMI Index and its problem, can actually be done to either approve or to disapprove the results of the study provided in this paper. [38]

ACKNOWLEDGEMENT

This work is supported by Directorate General of Higher Education Indonesia, as a part of Program Kompetisi Kampus Merdeka Research Grant to Binus University on 2021.

REFERENCES:

[1] ISO/IEC, "Information technology - Security techniques - Information security management systems - Overview and vocabulary," *Iso/Iec*, vol. 2009, p. ISO/IEC 27000:2009(E), 2009.

[2] "Guide for conducting risk assessments," 2012, doi: 10.6028/NIST.SP.800-30R1.

[3] A. Sabani, H. Deng, and V. Thai, "Evaluating the performance of e-government in Indonesia: A thematic analysis," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1481, pp. 435–440, 2019, doi: 10.1145/3326365.3326422.

[4] A. Rokhman, "E-Government Adoption in Developing Countries; the Case of Indonesia," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 2, no. 5, pp. 228–236, 2011, [Online]. Available:

http://oru.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwXVy7CgIxEAzW2giKpT9wkuzmdfVhsDhBxP7Ia8vDwv_HzYkItlttNQ-YGSEQTrL7wwTjkraQXWJ-1dnoij5p5xRUW3OB1ncer3gb7Bj8ff3Dr7AVqzrvRAjnx3DpWmJsen5mGKY2jLwcvhGySRPmHqLK1hSQRXnmIkl9yeQwaY-4F5vYguPzaymYlYM4IrHDsDW.

[5] M. Sukmana and C. Meinel, "E-government and security evaluation tools comparisonfor Indonesian e-government system," *ACM Int. Conf. Proceeding Ser.*, pp. 96–103, 2016, doi: 10.1145/3026724.3026741.

[6] "INDEKS KAMI | bssn.go.id." https://bssn.go.id/indeks-kami/ (accessed Jun. 22, 2021).

[7] A. N. Singh, M. P. Gupta, and A. Ojha, "Identifying factors of 'organizational information security management,'" *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014, doi: 10.1108/JEIM-07-2013-0052.

[8] Pusat Operasi Keamanan Siber Nasional, "Laporan Tahunan Hasil Monitoring Keamanan Siber 2020," *Bul. Jendela Data dan Inf. Kesehat.*, pp. 29–33, 2021.

[9] "Cyber Crime Attempts in Indonesia Surge during Coronavirus Pandemic." https://go.kompas.com/read/2020/11/17/180248674/cyber-crime-attempts-in-indonesia-surge-during-coronavirus-pandemic (accessed Oct. 16, 2021).

[10] C. Okoli and K. Schabram, "A Guide to Conducting a Systematic Literature Review of Information Systems Research," *SSRN Electron. J.*, vol. 10, no. 2010, 2012, doi: 10.2139/ssrn.1954824.

[11] G. Concha and P. Suárez, "Analyzing the best practices of information security and protection of sensitive data in the context of e-government in Colombia and Chile," *ACM Int. Conf. Proceeding Ser.*, no. i, pp. 198–201, 2013, doi: 10.1145/2591888.2591922.

[12] "What Is The CIA Triad?" https://www.f5.com/labs/articles/education/what-is-the-cia-triad (accessed Jul. 07, 2021).

[13] C. Lin and X. R. Luo, "Toward a Unified View of Dynamic Information Security Behaviors: Insights from Organizational Culture and Sensemaking," *Data Base Adv. Inf. Syst.*, vol. 52, no. 1, pp. 65–90, 2021, doi: 10.1145/3447934.3447940.

[14] ISACA, "Implementation Guideline ISO/IEC 27001:2013," *Isaca*, p. 64, 2016, [Online]. Available: https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf.

[15] M. H. Khyavi and M. Rahimi, "The missing circle of ISMS (LL-ISMS)," *SIGMIS-CPR 2015 - Proc. 2015 ACM SIGMIS Conf. Comput. People Res.*, pp. 73–77, 2015, doi: 10.1145/2751957.2751972.

[16] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, Jan. 2019, doi: 10.1016/J.PROCS.2019.11.234.

[17] R. Goel, A. Kumar, and J. Haddow, "PRISM: a strategic decision framework for cybersecurity risk assessment," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 591–625, 2020, doi: 10.1108/ICS-11-2018-0131.

[18] G. Karokola, S. Kowalski, and L. Yngström, "Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models," *2011 Inf. Secur. South Africa - Proc. ISSA 2011 Conf.*, no. C, 2011, doi: 10.1109/ISSA.2011.6027525.

[19] J. L. Spears, H. Barki, and R. R. Barton, "Theorizing the concept and role of assurance in information systems security," *Inf. Manag.*, vol. 50, no. 7, pp. 598–605, 2013, doi: 10.1016/j.im.2013.08.004.

[20] E. E. Enaw and N. Check, "Information systems security audits in Cameroon's public administration," *ACM Int. Conf. Proceeding Ser.*, pp. 312–317, 2018, doi: 10.1145/3209415.3209425.

[21] E. A. Rigon, C. M. Westphall, D. R. Dos Santos, and C. B. Westphall, "A cyclical evaluation model of information security maturity," *Inf. Manag. Comput. Secur.*, vol. 22, no. 3, pp. 265–278, 2014, doi: 10.1108/IMCS-04-2013-0025.

[22] A. Rabii, S. Assoul, K. Ouazzani Touhami, and O. Roudies, "Information and cyber security maturity models: a systematic literature review," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 627–644, 2020, doi: 10.1108/ICS-03-2019-0039.

[23] F. H. Alqahtani, "Developing an Information Security Policy: A Case Study Approach," *Procedia Comput. Sci.*, vol. 124, pp. 691–697, Jan. 2017, doi: 10.1016/J.PROCS.2017.12.206.

[24] W. Paper and Advisera, "Clause-by-clause explanation of ISO 27001," pp. 1–25, 2020, [Online]. Available: file:///Volumes/SD_CACHE/dropbox_gmail/Dropbox/Library.papers3/Reports/2020/Unknown/2020.pdf%0Apapers3://publication/uuid/78CA00E4-8563-4394-A16A-14EBE23EC47E%0Ahttp://www.iso.org.

[25] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *TQM J.*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.

[26] J. Breier and L. Hudec, "Risk analysis supported by information security metrics," *ACM Int. Conf. Proceeding Ser.*, vol. 578, pp. 393–398, 2011, doi: 10.1145/2023607.2023673.

[27] M. Zaydi and B. Nassereddine, "A new comprehensive solution to handle information security governance in organizations," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1481, pp. 1–5, 2019, doi: 10.1145/3320326.3320382.

[28] T. Pereira and H. Santos, "Security metrics to evaluate organizational IT security," *ACM Int. Conf. Proceeding Ser.*, vol. 2014-Janua, pp. 500–501, 2014, doi: 10.1145/2691195.2691275.

[29] P. Balozian and D. Leidner, "Review of IS security policy compliance: Toward the building blocks of an IS asecurity theory," *Data Base Adv. Inf. Syst.*, vol. 48, no. 3, pp. 11–43, 2017, doi: 10.1145/3130515.3130518.

[30] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, p. 101747, May 2020, doi: 10.1016/J.COSE.2020.101747.

[31] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," *J. Inf. Secur. Appl.*, vol. 58, p. 102726, 2021, doi: 10.1016/j.jisa.2020.102726.

[32] C. C. Angolano, I. R. Guzman, M. S. Garmon, and C. J. Navarrete, "Information technology security task-technology fit based on the technology-to-performance chain theory," *SIGMIS-CPR'12 - Proc. 2012 Comput. People Res. Conf.*, pp. 17–25, 2012, doi: 10.1145/2214091.2214100.

[33] E. Yasasin, J. Prester, G. Wagner, and G. Schryen, "Forecasting IT security vulnerabilities – An empirical analysis," *Comput. Secur.*, vol. 88, p. 101610, 2020, doi: 10.1016/j.cose.2019.101610.

[34] H. Abbas, C. Magnusson, L. Yngstrom, and A. Hemani, "Addressing dynamic issues in information security management," *Inf. Manag. Comput. Secur.*, vol. 19, no. 1, pp. 5–24, 2011, doi: 10.1108/09685221111115836.

[35] S. Dzazali and A. H. Zolait, "Assessment of information security maturity: An exploration study of Malaysian public service organizations," *J. Syst. Inf. Technol.*, vol. 14, no. 1, pp. 23–57, 2012, doi: 10.1108/13287261211221128.

[36] E. Bergström, M. Lundgren, and Å. Ericson, "Revisiting information security risk management challenges: a practice perspective," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 358–372, 2019, doi: 10.1108/ICS-09-2018-0106.

[37] A. Panou, C. Ntantogian, and C. Xenakis, "RiSKi: A framework for modeling cyber threats to estimate risk for data breach insurance," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1325, 2017, doi: 10.1145/3139367.3139426.

[38] V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 645–662, 2020, doi: 10.1108/ICS-01-2020-0004.

[39] A. Poller, S. Türpe, and K. Kinder-Kurlanda, "An Asset to Security Modeling ? Analyzing Stakeholder Collaborations Instead of Threats to Assets Categories and Subject Descriptors," *New Secur. Paradig. Work.*, pp. 69–81, 2014.

[40] W. Sung and S. Y. Kang, "An empirical study on the effect of information security activities: Focusing on technology, institution, and awareness," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1282, pp. 84–93, 2017, doi: 10.1145/3085228.3085242.

[41] H. S. Rhee, Y. U. Ryu, and C. T. Kim, "Unrealistic optimism on information

security management," *Comput. Secur.*, vol. 31, no. 2, pp. 221–232, 2012, doi: 10.1016/j.cose.2011.12.001.

[42] Y. H. and H. J. Mark Evans, Leandros A. Maglaras, "Human behaviour as an aspect of cybersecurity assurance," *Secur. Commun. Networks*, vol. 5, no. June, pp. 422–437, 2012, doi: 10.1002/sec.

[43] S. M. Ho, M. Kaarst-Brown, and I. Benbasat, "Trustworthiness attribution: Inquiry into insider threat detection," *J. Assoc. Inf. Sci. Technol.*, vol. 69, no. 2, pp. 271–280, 2018, doi: 10.1002/asi.23938.

[44] Š. Orehek and G. Petrič, "A systematic review of scales for measuring information security culture," *Inf. Comput. Secur.*, vol. 29, no. 1, pp. 133–158, 2020, doi: 10.1108/ICS-12-2019-0140.

[45] J. Sun, P. Ahluwalia, and K. S. Koong, "The more secure the better? A study of information security readiness," *Ind. Manag. Data Syst.*, vol. 111, no. 4, pp. 570–588, 2011, doi: 10.1108/02635571111133551.

[46] M. Shakibazad and A. J. Rashidi, "New method for assets sensitivity calculation and technical risks assessment in the information systems," *IET Inf. Secur.*, vol. 14, no. 1, pp. 133–145, 2020, doi: 10.1049/iet-ifs.2018.5390.

[47] R. Rieke, J. Schütte, and A. Hutchison, "Architecting a security strategy measurement and management system," *Proc. Work. Model. Secur. MDsec 2012*, 2012, doi: 10.1145/2422498.2422500.

[48] J. M. Such, A. Gouglidis, W. Knowles, G. Misra, and A. Rashid, "Information assurance techniques: Perceived cost effectiveness," *Comput. Secur.*, vol. 60, pp. 117–133, 2016, doi: 10.1016/j.cose.2016.03.009.

[49] A. A. Ganin *et al.*, "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," *Risk Anal.*, vol. 40, no. 1, pp. 183–199, 2020, doi: 10.1111/risa.12891.

[50] B. Duncan and M. Whittington, "Compliance with standards, assurance and audit: Does this equal security?," *ACM Int. Conf. Proceeding Ser.*, vol. 2014-Septe, pp. 77–84, 2014, doi: 10.1145/2659651.2659711.

[51] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, 2014, doi: 10.1016/j.cose.2014.04.005.

[52] H. Vescent and B. Blakley, "Shifting paradigms: Using strategic foresight to plan for security evolution," *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3285002.3285013.

[53] S. Fenz and T. Neubauer, "Ontology-based information security compliance determination and control selection on the example of ISO 27002," *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 551–567, 2018, doi: 10.1108/ICS-02-2018-0020.

[54] C. Everett, "Is ISO 27001 worth it?," *Comput. Fraud Secur.*, vol. 2011, no. 1, pp. 5–7, 2011, doi: 10.1016/S1361-3723(11)70005-7.

[55] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B. T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Comput. Secur.*, vol. 67, pp. 35–58, 2017, doi: 10.1016/j.cose.2017.02.005.

[56] Y.-S. Yen, "Information & Computer Security Article information :," *Inf. Comput. Secur.*, vol. 23, no. 2, pp. 145–160, 2015.

[57] W. Semple, "A threat-based approach to security," *Comput. Fraud Secur.*, vol. 2015, no. 2, pp. 7–10, 2015, doi: 10.1016/S1361-3723(15)30007-5.

[58] J. Fielding, "Back to basics: tackling security threats in an increasingly complex world," *Comput. Fraud Secur.*, vol. 2019, no. 7, pp. 6–8, 2019, doi: 10.1016/S1361-3723(19)30072-7.

[59] M. Jouini, L. B. A. Rabai, and R. Khedri, "A Multidimensional Approach towards a Quantitative Assessment of Security Threats," *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 507–514, Jan. 2015, doi: 10.1016/J.PROCS.2015.05.024.

[60] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *J. Inf. Secur. Appl.*, vol. 18, no. 1, pp. 45–52, 2013, doi: 10.1016/j.jisa.2013.07.002.

[61] D. Rios Insua, A. Couce-Vieira, J. A. Rubio, W. Pieters, K. Labunets, and D. G. Rasines, "An Adversarial Risk Analysis Framework for Cybersecurity," *Risk Anal.*, vol. 41, no. 1, pp. 16–36, Jan. 2021, doi: 10.1111/RISA.13331.

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

[62] G. Gonzalez-Granadillo *et al.*, "Automated cyber and privacy risk management toolkit," *Sensors*, vol. 21, no. 16, Aug. 2021, doi: 10.3390/S21165493.

[63] P. Tubío Figueira, C. López Bravo, and J. L. Rivas López, "Improving information security risk analysis by including threat-occurrence predictive models," *Comput. Secur.*, vol. 88, p. 101609, 2020, doi: 10.1016/j.cose.2019.101609.

[64] E. Rostami, F. Karlsson, and S. Gao, "Requirements for computerized tools to design information security policies," *Comput. Secur.*, vol. 99, p. 102063, Dec. 2020, doi: 10.1016/J.COSE.2020.102063.

[65] L. Allodi and F. Massacci, "Security Events and Vulnerability Data for Cybersecurity Risk Estimation," *Risk Anal.*, vol. 37, no. 8, pp. 1606–1627, 2017, doi: 10.1111/risa.12864.

[66] J. B. and A. Mostashari, "Measuring Systems Security," *Syst. Eng.*, vol. 14, no. 3, pp. 305–326, 2012, doi: 10.1002/sys.

[67] C. A. SARASTI, "What do we know about cyber risk and cyber risk insurance?" *Ekp*, vol. 13, no. 3, pp. 1576–1580, 2015.

[68] T. Waterbury, "Collective information structure model for Information Security Risk Assessment (ISRA)," *Eletronic Libr.*, vol. 34, no. 1, pp. 1–5, 2018.

[69] M. Nicho, "A process model for implementing information systems security governance," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 10–38, 2018, doi: 10.1108/ICS-07-2016-0061.

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

APPENDIX: TABLES

Table 3: Number of authors and affiliated institution based on country

Country	# Institution	% Institution	# Authors	% Authors
Slovakia	1	0.92%	2	1.12%
Bahrain	3	2.75%	4	2.23%
USA	22	20.18%	36	20.11%
Slovenia	1	0.92%	2	1.12%
Italy	6	5.50%	11	6.15%
Sweden	7	6.42%	10	5.59%
Malaysia	7	6.42%	8	4.47%
India	2	1.83%	3	1.68%
UK	6	5.50%	13	7.26%
Greece	8	7.34%	13	7.26%
Sussex	1	0.92%	1	0.56%
Iran	3	2.75%	4	2.23%
Canada	5	4.59%	5	2.79%
Netherlands	2	1.83%	3	1.68%
Lebanon	1	0.92%	1	0.56%
Singapore	2	1.83%	6	3.35%
Morocco	2	1.83%	5	2.79%
South Korea	5	4.59%	9	5.03%
Austria	2	1.83%	3	1.68%
Germany	6	5.50%	12	6.70%
South Africa	1	0.92%	1	0.56%
Portugal	2	1.83%	2	1.12%
Scotland	1	0.92%	2	1.12%
Pakistan	1	0.92%	2	1.12%
Australia	3	2.75%	6	3.35%
Spain	5	4.59%	9	5.03%
Tunisia	2	1.83%	2	1.12%
Indonesia	2	1.83%	4	2.23%
Total: 28 Countries	**109**		**179**	

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

Table 4: Selected study that covers Social aspect of IS

TITLE	SUMMARY
AN ASSET TO SECURITY MODELING? ANALYZING STAKEHOLDER COLLABORATIONS INSTEAD OF THREATS TO ASSETS[39]	This paper proposes a unique paradigm that security should be analyze not by the threat to asset but through measuring the performance of collaboration with stakeholders in which a risk to a system can be quickly addressed so that a mitigation can be implemented sooner.
THE MISSING CIRCLE OF ISMS (LL-ISMS)[15]	Provide some insight regarding ISMS in a social perspective. Called LL-ISMS or Low-Level ISMS, in which instead of focusing the workflow in technical side (PDCA), it focusses on the cooperation between actors in organization in which the workflow is defined as Do-Help-Feel-Think.
REVIEW OF IS SECURITY POLICY COMPLIANCE: TOWARD THE BUILDING BLOCKS OF AN IS SECURITY THEORY[29]	Provides some analysis regarding organization's actors compliance towards infosec policy, particularly staff members. This paper contains a deep study regarding motives, types of insiders, factors and any of the likes.
AN EMPIRICAL STUDY ON THE EFFECT OF INFORMATION SECURITY ACTIVITIES: FOCUSING ON TECHNOLOGY, INSTITUTION, AND AWARENESS[40]	Provide a study regarding the information security activities in general. This paper later provides some suggestion regarding infosec which consist of basically a connection between socio-technical aspect in organization that needs to be properly established, mainly the socio one based on the paper
UNREALISTIC OPTIMISM ON INFORMATION SECURITY MANAGEMENT[41]	This paper study the tendencies of MIS executive to feel denial of the risk. This paper proof that human or social factor is the second important in infosec management
HUMAN BEHAVIOR AS AN ASPECT OF CYBERSECURITY ASSURANCE[42]	This paper study the human factor to cyber security assurance based on a few case studies within this paper. It also proposes a framework that handles human factor to information security
TRUSTWORTHINESS ATTRIBUTION: INQUIRY INTO INSIDER THREAT DETECTION[43]	This paper study the behavioral of betrayer as an insider's threat in organization. This paper analyzes and make a framework to detect the behavior pattern with the use of "Human Sensor".
A SYSTEMATIC REVIEW OF SCALES FOR MEASURING INFORMATION SECURITY CULTURE[44]	this paper identifies and give an overview regarding different variables that can be used to measures infosec culture in organization.
IDENTIFYING FACTORS OF "ORGANIZATIONAL INFORMATION SECURITY MANAGEMENT"[7]	This paper identifies all the factors related to management in the context in infosec, further this paper argued that many organizations don't put too much attention regarding this sector in their infosec implementation.
THE MORE SECURE THE BETTER? A STUDY OF INFORMATION SECURITY READINESS[45]	This paper study the user attitudes towards IS compliance in organization

Table 5: Selected study that covers technical aspect of IS

TITLE	SUMMARY
INFORMATION TECHNOLOGY SECURITY TASK-TECHNOLOGY FIT BASED ON THE TECHNOLOGY-TO-PERFORMANCE CHAIN THEORY[32]	This paper evaluates the existing technologies for information security management and decide whether a technology is still relevant and effective in alleviating a risk which TLDR; depends on the IT guy who's using the technology.
FORECASTING IT SECURITY VULNERABILITIES – AN EMPIRICAL ANALYSIS [33]	This paper provides a methodology to forecast it-security vulnerabilities for post-release system and software implemented in organization. This paper also reviews its used metrics for the forecast which test the appropriateness of it.
EVALUATING THE CYBER SECURITY READINESS OF ORGANIZATIONS AND ITS INFLUENCE ON PERFORMANCE[31]	This paper study the different factors of cyber security readiness in organizations and how that factors affect its performance both financially and non-financially.

NEW METHOD FOR ASSETS SENSITIVITY CALCULATION AND TECHNICAL RISKS ASSESSMENT IN THE INFORMATION SYSTEM[46]	This paper proposes a new method to analyze, identified, and measure a risk based on its impact to informational assets. It also provides a framework to conduct a technical risk assessment.

Table 6: Selected study that covers the management aspect of IS

TITLE	SUMMARY
SECURITY METRICS TO EVALUATE ORGANIZATIONAL IT SECURITY [28]	This paper provides some insight regarding security metrics in organization, tackle the question of what vulnerabilities they should prioritize and accept so that it is cost efficient
A COMPREHENSIVE MODEL OF INFORMATION SECURITY FACTORS FOR DECISION-MAKERS [30]	This paper provides some in-depth explanation and to create a broad context regarding information security surface for decision maker.
ASSESSMENT OF INFORMATION SECURITY MATURITY: AN EXPLORATION STUDY OF MALAYSIAN PUBLIC SERVICE ORGANIZATIONS [35]	This paper study the same aspect of infosec as Singh2014, the management side to infosec.
REVISITING INFORMATION SECURITY RISK MANAGEMENT CHALLENGES: A PRACTICE PERSPECTIVE [36]	This paper identifies the challenges to infosec risk management. This paper revisit previous work that discuss the same topic, so this paper serves as the updated version of it
ADDRESSING DYNAMIC ISSUES IN INFORMATION SECURITY MANAGEMENT [34]	This paper provides a framework that deals with general problem in IS such as: Infosec externalities, dynamic security requirements management and ongoing evaluation/re-evaluation for IT services. The framework itself provide an automated strategic guidance that is tailored to the organization to solve these problems.

Table 7: Comparison table of the models found in the study

MODELS	EVALUATE TECHNICAL ASPECT	EVALUATE SOCIAL ASPECT	EVALUATE MANAGEMENT ASPECT	PROVIDE IMPROVEMENT PLAN	MATURITY EVALUATION	STANDARDS USED
KAMI INDEX [6]	YES	YES	YES	NO	YES	ISO27001
PRISM [17]	YES	YES	YES	YES	YES	ISO27001,NIST,COBIT
J. BREIER [26]	YES	YES	YES	NO	NO	ISO27002
R. RIEKE ET AL.[47]	YES	NO	YES	NO	NO	ISO27004, ISO27001
W. ABBAS [34]	YES	NO	NO	NO	NO	NONE
J. SUCH ET AL.[48]	YES	YES	YES	YES	NO	ISO27001, NIST
A. GANIN ET AL. [49]	YES	YES	YES	NO	NO	NONE
M. SHAKIBAZAD ET AL. [46]	YES	NO	NO	NO	NO	NONE
E. RIGON ET AL [21]	YES	YES	YES	YES	YES	ISO27001,27002,27005, COBIT