ISSN 2278-3091

Volume 8, No.1.5, 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse3581.52019.pdf

https://doi.org/10.30534/ijatcse/2019/3581.52019

Information Security Governance in Small Cities in Developing Countries

Johan Reimon Batmetan[1], Quido Conferti Kainde[2], Muhammad Nur[3],Trudi Komansilan[4],Sondy Kumajas[5]

[1]Information Technology and Communication Education Department, Universitas Negeri Manado, Indonesia
john.reimon@unima.ac.id

[2]Information Engineering Department, Universitas Negeri Manado, Indonesia, Email: quidokainde@unima.ac.id

[3]Universitas Muhammadiyah Sidenreng Rappang, Indonesia, Email: m.nurcokro@gmail.com

[4]Information Technology and Communication Education Department, Universitas Negeri Manado, Indonesia,
trudikomansilan@unima.ac.id

[5]Information Engineering Department, Universitas Negeri Manado, Indonesia, sondykumajas@unima.ac.id

ABSTRACT

Small cities in developing countries really need information that is safe and fast. Information security is very important in managing small cities in developing countries. Information technology is the best solution in managing information quickly and easily but is safe in its use. The purpose of this study is to analyze the condition of information security governance in small cities. This research uses measurement methods based on Information Security Governance, Information Security Risk Management, Information Security Management Framework, Information Asset Management, Technology, and Information Security. The results of this study indicate that security governance in small cities is still low and requires serious and comprehensive security improvements. The results of this study also found that the low level of information security management resulted in serious information security threats due to the low level of information security management. Serious ways and handling are needed to reduce time to do something, improve effectiveness, improve service information, introduce new services, increase the level of trust in investigating requests and services, facilitate services received, establish communication with users and improve service quality in small cities in the country developing.

Key words: information security, governance, small cities

1. INTRODUCTION

Information technology has become the best solution to running a modern organization. Information technology is used to capture, input, and process information quickly and easily. This makes the organization more efficient and effective in carrying out its organizational strategy. A comprehensive management model is needed so that it can result in the smart utilization of information technology especially in big cities[1]. The impact is that organizations become more competitive in carrying out their organizations. Technology has transformed many traditional organizations into modern, competitive and modern organizations. Modern organizations are very important to pay attention to information security in carrying out managing organizational systems[2]. In organizations that have used information technology as an enabler in their entire organizational system, information security is a very important thing to consider. Organizations need a special technique or model to manage the security of information to remain secure[3]. Organizations need to implement security system protection against all technology systems that they use.

Information security becomes one thing that is very important for organizations, especially government organizations or institutions. This is caused by the information collected relating to the community and national security. To manage an information security system, an organization must have a well-tested security standard by an institution that has the means to test and establish a security standard and be implemented properly[4]. In developed countries, information security standards have been set and required in all government institutions and audits are carried out rigorously and seriously so that the quality of the security system is reliable. But in developing countries (like Indonesia), information security systems still have limitations in implementing a strict information security system. This is due to the high costs involved in implementing an information security system and also the limited human resources that manage it. Another thing to consider is the low availability of information technology infrastructure and reduced convenience and long bureaucracy resulting in the difficulty of implementing information security systems in developing countries[5]. The difficulty of implementing a standardized information security system makes government institutions only provide limited information and the difficulty of securing the information on a large scale. Many government institutions only apply practical experience and knowledge in dealing with various jobs in information security systems.

Information security in government institutions becomes very important in the world of information technology. This is related to efforts to secure information assets from various threats that appear. Information security is very important to ensure the continuity of an institution's operations, optimize investment value and reduce risks that can occur both directly and indirectly[6]. Potential information security threats can be caused by the amount of information being managed. Clear boundaries are needed to build information that is safe, able to distinguish information that is accessible to the public and information that is confidential and is part of national security[7]. The threat can be damage, loss or spread of information to unwanted external parties. Information security systems are used to prevent unauthorized access in the form of program changes, theft and physical damage to existing systems[8]. This requires policies, procedures, and technical measurements. Limitations in implementing information security systems have a direct impact on government institutions in developing countries[9]. Government institutions become less optimal in managing information when the information security system is inadequate[10]. For this reason, some government institutions (especially central government institutions that have a scale of service nationally) in developing countries, apply certified information security standards from credible institutions. However, the implementation of standardized information security systems is more difficult in developing countries because of high prices and high requirements. One strategy developed in developing countries is to run with minimum standards based on experience and input from information technology consultants. However, this will face a problem when dealing with information security incidents where institutions experience limitations in handling them and IT consultants are not always available if needed so it is difficult to handle incidents that arise[11]. To overcome this deficiency, we need a model of information security standards that is cheap and can be implemented in government institutions in developing countries. This strategy can be used if existing government institutions already have information technology infrastructure and have a security system that adopts this information security model. Although the strategy for implementing this information security model is effective, problems arise in purchasing licenses, which directly affect the budget available at the institution.

To overcome this problem, researchers have suggested the following strategy: an information security model that covers the whole institutional governance system and applies generally to all government institutions where a uniform model occurs so that it is easy to control and also the financing charged to an institution that is authorized to manage the governance system security[12]. This strategy is effective and can be implemented in government institutions in developing countries. However, several problems still arise that this information security model has not been able to explain in detail about the real condition of information security systems in an institution and user behavior in a realistic manner in developing countries. Furthermore, the applied information security model requires institutional compliance with a standard and internationally valid information security standard.

Therefore, this study aims to show the model of information security systems and analyze the conditions of information security governance in small cities in developing countries. Unlike other security systems, our security system model is specific to small cities in developing countries with information technology management that is cheap and easy to implement for each institution without having to have expensive information security standards and IT consultants who are always ready at all times. The novelty of this governance system is suitable for small cities in developing countries which have many financial limitations, low governance, and low processing resources. This model consists of the model of Governance, Risk Management, Framework, Asset Management, and Technology Aspects. This governance system is used because it is widely applied in many institutions.

2. LITERATUR REVIEW

Information security requires regular audits to ensure reliability for institutional continuity. Investigations conducted in the internal audit system are effective as a standard of governance and risk management in an institution[13]. This will guarantee the quality of audits conducted on information security systems. Risk management contributes to the information technology governance mechanism that is applied to the institution[14]. Information security is also influenced by several factors such as information user motivation, attitudes in sharing information, behavior, and norms in using information[15]. Security culture needs to be built based on factors of responsibility, trust, communication, co-operation in increasing awareness of information security systems[16]. Relationships among employees within an institution, the level of employee structure and the breadth of an institution's services can affect information security[17]. A way is needed to control the output of information to keep it confidential and good feedback[18].

An information security system requires an overall concept to carry out overall protection of the institutional work environment[19]. In general, information security aims to secure overall institutional assets. This has a cycle ranging from assets, design, implement, and maintain. The entire life cycle is described by awareness and training, policy and procedures, device management implementation, monitoring, incidents, incident response investigations, cybercrime and forensics, electronic discovery expert witnesses, reactive services, litigation support services[20].

Incidents that occur must be handled with appropriate procedures and quickly both handling and escalation of incidents that occur[4]. Frameworks and procedures are needed so that incidents that occur do not become a serious problem for the institution. Institutional-based knowledge is very important to build awareness of information security in developing a trusted institution[21]. Institutions need a policy that applies thoroughly to all employees in the use of various resources owned by the institution such as password management, email usage, internet use, social media, mobile computing, and handling information managed by the institution[22]. Awareness of information security has a positive effect on good password management. This also has a positive effect on personal information, and positively gives awareness to security threats to build strong passwords[23]. Information also really needs learner's attention, and self-efficacy to recognize the potential threats that will be faced such as cyber-attacks and phishing[24][25][26].

Awareness of information security makes government institutions use information technology to make things safer by revolutionizing the way e-government is more secure to use. Secure e-government has enabled government institutions to present information and services efficiently in a period and minimum cost. This research tries to see the extent to which government institutions carry out governance in the effectiveness of the formation of e-government. This is to increase effectiveness, improve service information, introduce new services, increase the level of trust in investigating requests and services, facilitate the services received, establish communication with users and improve service quality.

3. METHOD

The method used to measure the information security index has been tested and used by government institutions in Indonesia. This index is named the index KAMI (Keamanan Informasi = Information Security). This is caused by the information security factor in an organization/institution which is very important and should be the main concern. Our index has been tested and modified to meet the criteria for implementing information security in organizations that include completeness and maturity following standards. OUR Index is an application that is used as a tool to analyze and evaluate the level of readiness (completeness and maturity) of the application of information security in an organization following the criteria in SNI ISO / IEC 27007, namely: Governance, Risk Management, Framework, Asset Management, Technology Aspects as shown in Figure 1.

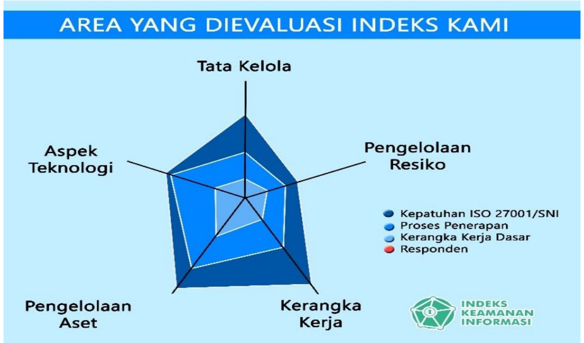


Figure 1: KAMI Index Area

The KAMI Index is not intended to analyze the feasibility or effectiveness of existing forms of security, but rather as a tool to provide an overview of the readiness of the information security framework to the Institution Leaders. The implementation of the KAMI Index is carried out by public service providers electronically through Technical Guidance, Assessment, and Consultation.

The Information Security Readiness Evaluation Phase in this section will explain the flow in the second stage, namely the information security readiness evaluation phase as follows:

1) Define the scope The first step of the evaluation that must be done is to define the scope of the assessment. The scope can be chosen following the interests of the KAMI Index assessment and can be chosen as a work unit (at any level) or an information system.
2) Determine the role or level of importance in the institution Before the assessment process is carried out quantitatively, the classification process is carried out first on the role of ICT in the agency or the scope of its evaluation. Respondents were also asked to briefly describe the existing ICT infrastructure in their work units. The purpose of this process is to group agencies into specific "sizes": Low, Medium, High and Critical.
3) Assess the completeness of security in 5 areas. The assessment in KAMI Index is carried out with the overall coverage of the security requirements listed in the ISO / IEC 27001: 2009 standard, which is reorganized into the 5 (five) areas below:
    a. Information Security Governance evaluates the readiness of information security governance forms along with the agencies/ functions, duties, and responsibilities of information security managers.
    b. Information Security Risk Management, evaluates the readiness of implementing information security risk management as the basis for implementing an information security strategy.
    c. Information Security Framework evaluates the

completeness and readiness of the information security management framework (policy & procedure) and its implementation strategy.

d. Management of Information Assets evaluates the completeness of security of information assets, including the entire cycle of use of those assets; and

e. Information Technology and Security, evaluates the completeness, consistency, and effectiveness of the use of technology in securing information assets.

The sampling technique was by distributing questionnaires to employees totaling 500 respondents in 100 Indonesian government institutions and categorized as small cities. The distribution of questionnaires uses information and communication technology, which is surveyed to measure the level of maturity. Data were analyzed in the form of questionnaires using the KAMI Index. The formation of e-government reduces the time to do something, increases effectiveness, improves service information, introduces new services, increases the level of trust in investigating requests and services, facilitates services received, establishes communication with users and improves service quality. In analyzing data through the results of respondents (questionnaire) to measure the level of maturity of E-Governance so that the results have been obtained to what extent the maturity and security of information systems are implemented in government agencies.

4. RESULT AND DISSCUSION

The results of this study are divided into six assessment indices, namely: Part 1: Electronic Systems Category, Part 2: Information Security Governance, Part 3: Management of Information Security Risks, Part 4: Framework for Information Security Management Framework, Part 5: Management of Information Assets, Part 6: Information Technology and Security. The results we get are wherein Information Security the results of Table 1 and figure 2.

Table 1: Information Security Questionnaire

ASSESSMENT INDEX	**questionnaire respondent**				
	I	**II**	**III**	**IV**	**V**
Electronic system	25	28	25	27	14
Governance	126	43	89	114	24
Risk Management	48	34	51	48	18
Information Security Framework	152	62	125	152	32
Asset Management	82	90	143	82	82
Information Technology and Security	80	80	103	80	80

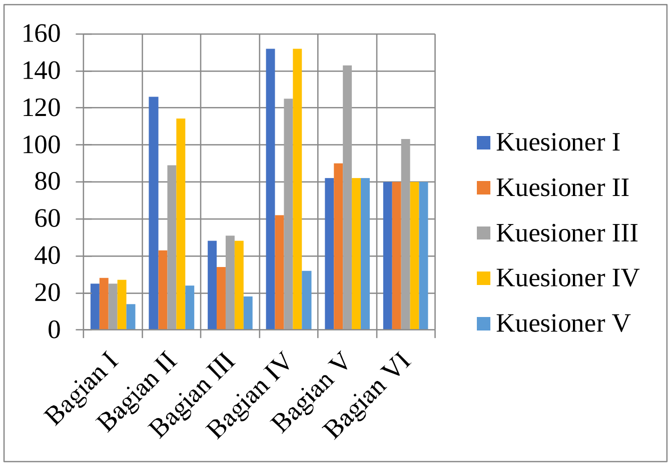
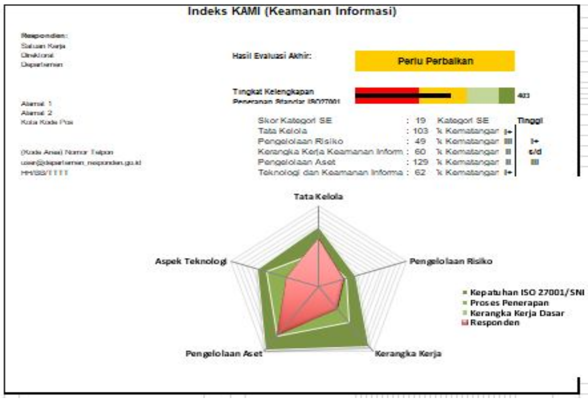


Figure 2: Information Security Questionnaire.

The results of the study conducted, researchers used the KAMI index which is divided into six categories. In the first category, the KAMI Index measures electronic systems, where this section evaluates the level of electronic systems used. This electronic system level consists of low, high and strategic categories. The results of this study indicate that the level of application of electronic systems is in the high category which means that it is still in a medium condition with a total score of 19. The measurement results show that government institutions in developing countries only have an investment value in electronic systems under IDR 3 billion and enter into the low area. This means that government institutions invest very little in the electronic systems used. This is caused by electronic systems that are not yet a priority. On the other hand, operational funds are only around less than IDR 1 billion to run the electronic system. The average government institution has not applied and obeyed certain rules or standards and is still running as it is according to the leadership's instructions so that the system is very dependent on the institutional leader. On the information security side, the system being run also has not implemented a special security algorithm to secure the system being run. The system is still running as is without applying special security. The number of users running an electronic system is also still limited, averaging only 5000 users. Data that is managed on an electronic system is also still an ordinary data which has a relatively ordinary level of criticality against the threat of hacking, attacking or breaking through information security. This means that electronic systems in government institutions have not yet implemented a strong security system and are still managing data that is public and commonly accessed by the public. This is since several applications are directly managed by central agencies whose information security is more guaranteed nationally than in the regions. The usual level of criticism in question is a process that does not risk disrupting the lives of many people and does not directly impact the government-managed system. This means that many systems managed by the government are not run electronically but conventionally without electronic systems. This can be seen if an electronic system has a system failure, so the impact is not widespread nationally and does not endanger national security and defense. The potential loss or negative impact of incidental penetrating electronic information system security (eg sabotage, terrorism, etc.) only impacts temporary operational disruptions and does not endanger lives or large financial losses. See figure 3.



Indeks KAMI (Keamanan Informasi)

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Hasil Evaluasi Akhir: Perlu Perbaikan

Tingkat Kelengkapan Penerapan Standar ISO27001 403

```
Skor Kategori SE                  :  19   Kategori SE      Tinggi
Tata Kelola                       : 103   Tk Kematangan  I+
Pengelolaan Risiko                :  49   Tk Kematangan  III   I+
Kerangka Kerja Keamanan Inform    :  60   Tk Kematangan  II    s/d
Pengelolaan Aset                  : 129   Tk Kematangan  II    III
Teknologi dan Keamanan Informa    :  62   Tk Kematangan  I+
```

Figure 3: Results of governance recapitulation

The second part of information security governance, this section evaluates the readiness of information security governance forms and their agencies or functions, duties and responsibilities, information security management. The results are displayed in the form of assessments not carried out, in planning, in the application or partially applied, applied in their entirety. The results of this study indicate that in principle or responsibility for the implementation of information security programs including the establishment of policies has been carried out thoroughly in government institutions. Institutions also have functions or sections that specifically have the responsibility of managing information security and maintaining compliance. This is only expected in some existing functions, especially those that have not been done online. The resources assigned to be responsible for securing information are not following their duties and functions, so they do not guarantee compliance with available security standards. The results of this study also show that the role of implementing information security covering all needs has not been mapped completely, including the need for internal audit and the requirements for the segregation of authority so that there are still many shortcomings. This is caused by government agencies not defining the requirements/standards of competence and expertise in implementing information security management. Another thing is that all the implementers of information security in government agencies do not yet have adequate competence and expertise following applicable requirements/standards. Government agencies have implemented a part of the awareness-raising and understanding program for information security, including the importance of compliance for all parties involved. Agencies also only implement a part of the competency and expertise improvement program for officials and implementing officers in managing information security. So only a few of them are participating in the program and still have limited competence.

The results of this study indicate that government agencies have not integrated the requirements for information security in the existing work processes. Government agencies are still limited to planning to identify personal data used in work processes and implementing safeguards following applicable laws and regulations. This is because the laws relating to private data are not yet available so they are still limited. Information security management responsibilities include coordination with internal and external information asset managers/users as well as other interested parties, to identify security requirements (for example information exchange or cooperation involving important information) and to resolve existing problems, as a whole. This is the same as information security managers who proactively coordinate with relevant work units (HR, Legal / Legal, General, Finance, etc.) and external parties concerned (eg regulators, security forces) to implement and ensure compliance with information security related to work processes that involve various parties carried out thoroughly. The responsibility for deciding, designing, implementing and managing steps for the continuation of ICT services (business continuity and disaster recovery plans) has been defined and allocated is still done in a limited and only part of it. The person responsible for managing information security reports the condition, performance/effectiveness and compliance of the information security program to the leadership of the Agency on a regular and comprehensive basis. The conditions and information security issues at your agency become a consideration or part of the strategic decision-making process at the agency carried out in some functions only. The leadership of the work unit in the government agency implements a special program to adhere to the goals and objectives of compliance with information security, specifically covering the information assets for which they are responsible for being implemented as a whole.

Government agencies still apply in part to defining metrics, parameters, and processes for measuring the performance of information security management which includes the mechanism, measurement time, implementation, monitoring and escalation of reporting. Government agencies are still planning to implement an information security management performance evaluation program for the individual (officials & officers) implementing it. Government agencies have implemented several targets and targets for information security management in various relevant areas, evaluating their achievements regularly, implementing corrective measures to achieve existing targets, including reporting on their status to Agency leaders. Government agencies are still planning to identify legislation, legal instruments and other standards related to information security that must be complied with and analyze the level of compliance. Government agencies still do partly by defining policies and measures to deal with information security incidents involving violations of the law (criminal and civil). Conclusions that can be made in the governance section, government agencies only have a low level of maturity with a total score of 79. Overall seen in table 2.

Table 2: Recapitulation of information security index assessment results

Category	Score	Results
Electronic system	19	High
Governance	103	Maturity Level: I +
Risk Management	49	Maturity Level: III
Information Security Framework	60	Maturity Level: II
Asset Management	129	Maturity Level: II
Information Technology and Security	62	Tk Maturity : I+

In the information security risk management section, this study evaluates the readiness for implementing information security risk management as the basis for implementing an information security strategy. Evaluation results are made in the Not Done category; In Planning; In Application or Partially Implemented; Applied Thoroughly. The results of this study indicate that government agencies have a documented information security risk management work program that is officially used only in some functions. The government agency has also assigned the person in charge of risk management and escalating the reporting status of information security risk management to the leadership level and is carried out thoroughly. Government agencies do not yet have a documented information security risk management framework that is officially used but has plans to act on it. This risk management framework includes the definition and relationship of the level of classification of information assets, the level of threat, the likelihood of the threat occurring and the impact of losses on your Agency and is still determined in the planning. Government agencies have set a threshold level of risk that can be accepted as a whole. Government agencies have also defined ownership and management (custodian) information assets that exist, including the main/important assets and the main work processes that use these assets and only partially implemented. Threats and weaknesses related to information assets, especially for each main asset have been identified and only partially indicated. The impact of losses related to the loss/disruption of the function of the main assets has been determined following the existing definition. Government agencies have carried out structured information security risk analysis/analysis initiatives on existing information assets (to be used later in identifying mitigation or countermeasures that are part of the information security management program) of some existing assets. Government agencies have compiled some of the mitigation and risk management measures that are available but are incomplete. Risk mitigation measures are arranged in part according to priority levels with targets for completion and those responsible for them, by ensuring the effective use of resources that can reduce risk levels to an acceptable threshold by minimizing the impact on ICT service operations. The status of completion of risk mitigation measures is monitored regularly, to ensure completion or progress of work in only a few functions. Completion of mitigation measures that have been applied to some functions is evaluated, through an objective / measurable process to ensure consistency and effectiveness. The risk profile along with its mitigation forms are periodically reviewed to ensure accuracy and validity, including revising the profile if there are significant changes in conditions or the need for the application of new safeguards to be applied comprehensively in each section. The planning risk management framework is regularly reviewed to ensure/improve its effectiveness and is still in planning. Risk management is part of the objective assessment process of the performance of security effectiveness is still being carried out in the planning so that government agencies are still at risk in overcoming and mitigating the risks that arise. Conclusions that can be reached in the management of information security risks, government agencies are still at the level III maturity level with a value of 49 and are still high risk.

In the information management framework, the researcher evaluates the completeness and readiness of the information security management framework and its implementation strategy. The results of the assessment are made in the category of Not Performed, In Planning, In Application or Partially Implemented, and in All-Applied. This section is divided into two parts. First, the Formulation and Management of Information Security Policies & Procedures. The policies and procedures, as well as other documents required regarding information security, have been prepared and written clearly, by stating the roles and responsibilities of the parties who are given the authority to implement them have been implemented thoroughly. The information security policy is still in the plan to be formally established, published to all staff/employees including related parties and easily accessed by those who need it. Government institutions have applied to some functions or sections to provide mechanisms for managing information security policy documents and procedures, including the use of a master list, distribution, withdrawal from circulation and storage. Processes (including implementers, mechanisms, schedules, materials, and targets) for communicating information security policies (and changes) to all relevant parties, including third parties, have been applied to some of the available functions. All existing information security policies and procedures reflect the need for mitigation from the results of the information security risk assessment, as well as specific objectives/objectives set by the leadership of the Agency and partially implemented. Processes are available to identify conditions that jeopardize the security of information and designate them as information security incidents to be followed up following procedures that are applied comprehensively to the institution. Information security aspects which include incident reporting, maintaining confidentiality, intellectual property rights, rules for the use and security of ICT assets and services listed in contracts with third parties are still in the planning. Government institutions have implemented it thoroughly by considering the consequences of violations of information security policies that have been defined, communicated and enforced. Partially implemented and official procedures are in place to manage exceptions to the application of information security, including processes to follow up on the consequences of this condition.

Government organizations are still planning to implement operational policies and procedures to manage the implementation of security patches, allocation of responsibilities to monitor the release of new security patches, ensure their installation and report on them. Government organizations have also applied in part to discuss aspects of information security in project management related to scope. Government organizations are already planning to implement a process for evaluating risks related to the planned purchase (or implementation) of a new system and addressing the problems that arise. Government organizations have also planned to implement a secure system development process (Secure SDLC) using principles or methods according to the technology platform standards used. The implementation of a system results in new risks or non-compliance with existing policies, is there a process to overcome this, including the application of new security (compensating control) and the complete schedule for some existing functions. A plan has been made for the availability of a business continuity planning (ICT) continuity planning management framework that defines information security requirements/considerations, including the scheduling of trials. Planning is made for disaster recovery of ICT (disaster recovery plan) services that have defined the composition, roles, authority, and responsibilities of the designated team. Planning has also been carried out for the trial of disaster recovery planning for ICT (disaster recovery plan) services that have been carried out according to schedule. In addition, planning is also carried out for the results of disaster recovery planning for ICT (disaster recovery plan) services that are evaluated to implement the necessary corrective or corrective measures (for example, if the results of trials show that the recovery process cannot (fail) to meet the existing requirements All information security policies and procedures are regularly evaluated for eligibility and carried out in careful planning.

Second, Management of Information Security Strategies and Programs, government institutions have planned to have a strategy for implementing information security following the results of a risk analysis which is implemented as part of an organization's work plan. Government organizations already have a strategy for using information security technology, whose application and update is tailored to the needs and changes in the risk profile that is applied to some functions. Information security implementation strategy is realized as part of the implementation of work programs in some organizational functions. Government organizations have and carry out internal audit programs conducted by independent parties with the overall scope of information assets, existing security policies and procedures (or following applicable standards) and applied to the organization as a whole. The internal audit evaluates the level of compliance, consistency, and effectiveness of the application of information security and is applied to some installed systems. The results of the internal audit are reviewed/evaluated to identify corrective and preventive measures, or information security performance improvement initiatives are applied only to some functions of the organization. The results of the internal audit are reported to the leadership of the organization to establish corrective measures or programs to improve information security performance and apply only to the part of the audit. If there is a need to revise the policies and procedures that apply, then a comprehensive analysis is carried out to assess the financial aspects (impact of costs and budget requirements) or changes to infrastructure and management of changes, as a precondition for implementing it. Government organizations periodically examine and evaluate the level/status of compliance with existing information security programs (including exceptions or other conditions of non-compliance) to ensure that all of these initiatives, including the necessary corrective measures, have been effectively implemented and applied only to some functions of the organization. Government organizations have plans and programs to improve information security for the medium / long term (1-3-5 years) that are realized consistently and carried out thoroughly. From the results of research conducted, found in this section score 60 and only be in level II level of maturity. This shows that government organizations in developing regions are still low by only having standards but not yet implementing them properly. Steps are still needed to improve the ability to deal with information security problems.

In this section, the sections relating to the management of information assets are examined. This section evaluates the completeness of securing information assets, including the entire cycle of use of these assets. The assessment is carried out in the category of Not Performed, In Planning, In Application or Partially Implemented, Completely Applied. The results of this study are divided into two parts, the first part is the management of information assets. The results of this study indicate that a comprehensive inventory list of information assets and assets related to the information technology process is complete, accurate and maintained (including asset ownership). There is a definition of information asset classification following applicable laws and regulations and applies to all organizational structures. Government organizations also carry out a whole process to evaluate and classify information assets according to the level of importance of the assets for the Agency and its security needs. For information systems, there are definitions of different levels of access from each classification of information assets and matrices that record the allocation of access and are applied in part. Government organizations do not make processes of managing changes to systems, business processes and information technology processes (including configuration changes) that are applied consistently. This becomes a weakness that must be corrected. The availability of a configuration management process that has been applied consistently has been carried out in part. The availability of the process to release a new asset into the operational environment and update the inventory of information assets has been implemented thoroughly. The command agency owns and applies the tools below, as a continuation of the process of implementing risk mitigation. This can be seen in the definition of information security responsibilities individually for all personnel in government agencies that are applied as a whole.

The rules for the use of computers, e-mail, internet, and intranet have been partially implemented. The rules for securing and using assets of institutions related to intellectual property rights have been established comprehensively. Regulations regarding the installation of software in IT assets belonging to agencies are applied in part. But the government is still planning the use of personal data regulations that require the written permission of the owner of personal data. Electronic identity management and authentication processes (username & password) including policies on violations are applied in part. The requirements and procedures for managing/granting access, authentication and authorization to use information assets have been carried out thoroughly. The provisions regarding storage time for classification of existing data and conditions for data destruction are still only partially applied. Provisions regarding the exchange of data with external parties and safeguards are still carried out in part. The investigation/investigation process to resolve incidents related to information security failures has been carried out thoroughly. Procedures for regular back-up and trial of data restoration and physical security provisions that are adjusted to the definition of zones and the classification of assets contained therein have been carried out in some organizational functions. Several things have been carried out as a whole such as the process of checking HR background, the process of reporting information security incidents to external parties or authorities, and procedures for destruction of data/assets that are no longer needed. In the Procedure for the study of the use of access (user access review) and access rights (user access rights) following the steps to improve if there is a non-conformity (non-conformity) to the applicable policy has been done in part on the functions of the organization. While some things have been done thoroughly, such as procedures for users who are mutated / outgoing or contracted / outsourced workers who have expired, available lists of data / information that must be backed up and reports on analysis of compliance with their backup procedures, available list of records of security implementation information and forms of security in accordance with its classification. Procedure for using third-party information processing devices (including personal equipment and work partners/vendors) by ensuring aspects of intellectual property rights and securing access that is used is not carried out.

The second part discusses physical security. The measured part is a comprehensive implementation of security of physical facilities (work sites) that are following the interests/classification of information assets, in layers and can prevent access attempts by unauthorized parties as a whole. Besides, five other things that have been done as a whole are, there is a process to manage the allocation of entrance keys (physical and electronic) to physical facilities. Computational infrastructure is protected from environmental impacts or fire and is in a condition with temperature and humidity following the manufacturer's requirements. The installed computing infrastructure is protected from power supply disruptions or the effects of lightning. Security regulations for your agency's computing devices are available when used outside the official work location (office). A process is available to move ICT assets (software, hardware, data/information, etc.) from a predetermined location (in the inventory list). Processes are available to secure work locations from the presence/presence of third parties who work for the benefit of your agency. Whereas regulations are available to secure important work locations (server rooms, archive rooms) from the risk of devices or materials that can endanger information assets (including information processing facilities) that are in it (for example a ban on the use of mobile phones in server rooms, using cameras, etc.) are not done. The conclusion obtained in this section is the level of asset management is at the level of maturity level II with a value of 129. This is still relatively low and requires better improvement.

In the technology and information security section, evaluating the completeness, consistency, and effectiveness of the use of technology in securing information assets. Assessments are carried out by category, Not Done, In Planning, In

Application or Partially Implemented, Wholly Applied. ICT services (computer systems) that use the internet are protected with more than 1 layer of security implemented in part. The communication network is segmented according to its interests (a division of Agencies, application requirements, special access points, etc.) has been done thoroughly. The planning part is still available, such as a standard configuration for the system security for all network assets, systems and applications, which is updated according to developments (applicable industry standards) and needs, as well as government agencies routinely analyze compliance with the implementation of existing standard configurations. Networks, systems, and applications that are used routinely are scanned to identify possible vulnerabilities or changes/integrity of the configuration, and the overall network infrastructure, systems, and applications are designed to ensure availability (redundant design) according to the needs/requirements that still apply in part to the organization. Overall network infrastructure, systems, and applications are monitored to ensure the availability of sufficient capacity for existing needs is still being done in the planning. Every change in the information system is automatically recorded in the login part. Attempts to access by unauthorized parties automatically recorded in the log are not carried out by the organization.

Four things are still being done in planning: all logs are analyzed periodically to ensure the accuracy, validity, and completeness of their contents (for the sake of audit and forensic traces. Government agencies apply encryption to protect important information assets according to existing management policies. Government agencies have standards in use encryption Government agencies implement safeguards to manage encryption keys (including electronic certificates) that are used, including the usage cycle, all systems and applications automatically support and implement automatic password changes, including deactivating passwords, setting complexity/length and reuse old password is not done Access is used to manage the system (system administration) using a special form of layered security has been done in some organizations. Systems and applications used have implemented restrictions on access time. The process of automation of timeouts, lockouts after login failures, and withdrawal of access has been carried out thoroughly. Government agencies have implemented security measures to detect and prevent unauthorized use of network access (including wireless networks). Government agencies have thoroughly implemented special forms of security to protect access from outside the Agency. The operating system for each desktop and server device is updated with the latest version still partially done. Every desktop and server has been thoroughly protected from attacks by viruses (malware). Then there are five parts that have been applied to some organizations, namely the existence of records and analysis results (audit trail - audit trail) that confirms that antivirus / antimalware has been updated routinely and systematically, there are reports of attacks of viruses/malware that failed / successfully followed up and completed, the entire network, systems and applications have used an accurate time synchronization mechanism, in accordance with existing standards, agencies have implemented a development and trial environment that has been secured in accordance with existing technology platform standards and is used for the entire life cycle of the system being built. the government engages independent parties to regularly review the reliability of information security. Whereas each application has security specifications and functions that are verified/validated during the development and trial process are still being carried out in the planning. The conclusion in this section is that the level of maturity is only at a level I + with a value of 62 and belongs to the low category and is a much-needed improvement to build a better security system.

5. CONCLUSION

This study concludes that the information security system model and information security governance conditions in small cities in developing countries can be measured by the KAMI information security system model. This model can properly map the six categories of information security such as electronic systems used, governance, risk management, information security frameworks, asset management, and technology and information security. The results of this study conclude that the KAMI model can be used well to measure information security systems in government institutions in developing countries. The results of the measurement of information security systems at government institutions in developing countries that the security system still needs a thorough and serious improvement. Government institutions still have a low information security system and do not yet have good security standards and still need implementation in many parts of the organization and must be carried out thoroughly. Government institutions must adopt many secure and trusted information security systems.

REFERENCES

[1] N. Athirah, M. Asri, R. Ibrahim, and S. Jamel, "Designing a Model for Smart City through Digital Transformation," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.3, pp. 345–351, 2019. https://doi.org/10.30534/ijatcse/2019/6281.32019

[2] M. Nur, J. R. Batmetan, and H. K. Manggopa, "Smart City Maturity Level Analysis Using ITIL Framework," *Adv. Soc. Sci. Educ. Humanit. Res.*, vol. 299, no. Ictvet 2018, pp. 243–247, 2019. https://doi.org/10.2991/ictvet-18.2019.55

[3] J. P. Runtuwene, R. A. Mege, V. R. Palilingan, and J. R. Batmetan, "Information Security Awareness on Data Privacy in Higher Education," *Adv. Soc. Sci. Educ.*

Humanit. Res., vol. 299, no. Ictvet 2018, pp. 172–174, 2019.
https://doi.org/10.2991/ictvet-18.2019.38

[4] J. R. B. V R Palilingan, "Incident Management in Academic Information System using ITIL Framework Incident Management in Academic Information System using ITIL Framework," *IOP Conf. Ser. Mater. Sci. Eng. Pap.*, vol. 23, no. 2, 2018.

[5] V. R. Palilingan and J. R. Batmetan, "Competitive Intelligence framework for Increasing Competitiveness Vocational High School Management," *Adv. Soc. Sci. Educ. Humanit. Res.*, vol. 299, no. Ictvet 2018, pp. 230–233, 2019.

[6] J. Järveläinen, "International Journal of Information Management IT incidents and business impacts : Validating a framework for continuity management in information systems," *Int. J. Inf. Manage.*, vol. 33, no. 3, pp. 583–590, 2013.

[7] D. Witarsyah, I. Journal, D. W. Jacob, M. F. Fudzee, M. A. Salamat, and N. H. Ab, "Analyzing the Barrier to Open Government Data (OGD) in Indonesia," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.3, pp. 136–139, 2019.
https://doi.org/10.30534/ijatcse/2019/2681.32019

[8] M. Jäntti, "Defining Requirements for an Incident Management System : A Case Study," in *Fourth International Conference on Systems*, 2009, pp. 184–189.
https://doi.org/10.1109/ICONS.2009.17

[9] N. S. M. Mizan, M. Y. Ma, N. S. M. Satar, and S. M. Shahar, "CNDS-Cybersecurity : Issues and Challenges in ASEAN Countries," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.4, pp. 113–119, 2019.
https://doi.org/10.30534/ijatcse/2019/1781.42019

[10] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Comput. Secur.*, pp. 1–27, 2014.

[11] M. Marrone and L. M. Kolbe, "Uncovering ITIL claims : IT executives ' perception on benefits and Business-IT alignment," *Inf Syst E-Bus Manag.*, vol. 9, pp. 363–380, 2011.

[12] M. Marrone, F. Gacenga, and A. Cater-steel, "IT Service Management : A Cross-national Study of ITIL Adoption IT Service Management : A Cross-national Study of ITIL Adoption I . INTRODUCTION Management : A Cross-national Study of ITIL Adoption," *Commun. Assoc. Inf. Syst.*, vol. 34, pp. 865–892, 2014.
https://doi.org/10.17705/1CAIS.03449

[13] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure ! Designing information security awareness programs to overcome users ' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, pp. 145–159, 2017.

[14] P. John, R. L. Raschke, G. Gal, and W. N. Dilla, "Accounting , Organizations and Society The influence of a good relationship between the internal audit and information security functions on information security outcomes," *Accounting, Organ. Soc.*, 2018.

[15] N. S. Safa and R. Von Solms, "Computers in Human Behavior An information security knowledge sharing model in organizations," *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016.

[16] D. Ki-aries and S. Faily, "Persona-centred information security awareness," *Comput. Secur.*, vol. 70, pp. 663–674, 2017.
https://doi.org/10.1016/j.cose.2017.08.001

[17] D. Dang-pham, S. Pittayachawan, and V. Bruno, "Investigation into the formation of information security influence : Network analysis of an emerging organisation," *Comput. Secur.*, vol. 70, pp. 111–123, 2017.

[18] C. Xu, Y. Zhao, J. Zhang, and H. Qi, "System Identification under Information Security," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 3756–3761, 2017.
https://doi.org/10.1016/j.ifacol.2017.08.477

[19] A. Malyuk and N. Miloslavskaya, "Information Security and Expert ' s Knowledge Autoformalization," *Procedia - Procedia Comput. Sci.*, vol. 88, pp. 288–293, 2016.

[20] B. Rahardjo, *Keamanan informasi*. .

[21] A. Rahman, M. Lubis, and A. Ridho, "Information Security Awareness at the Knowledge-Based Institution : Its Antecedents and Measures," *Procedia - Procedia Comput. Sci.*, vol. 72, pp. 361–373, 2015.

[22] F. H. Alqahtani, "Developing an Information Security Policy : A Case Study Approach," *Procedia Comput. Sci.*, vol. 124, pp. 691–697, 2018.

[23] S. Mamonov and R. Benbunan-fich, "Computers in Human Behavior The impact of information security threat awareness on privacy-protective behaviors," *Comput. Human Behav.*, vol. 83, pp. 32–44, 2018.

[24] J. C. Sun and K. P. Yeh, "Computers & Education The effects of attention monitoring with EEG biofeedback on university students ' attention and self-efficacy : The case of anti-phishing instructional materials," *Comput. Educ.*, vol. 106, pp. 73–82, 2017.

[25] T. Hariguna, & Akmal,"Assessing students' continuance intention in using multimedia online learning", TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(1), 187–193, 2019. http://doi.org/10.12928/TELKOMNIKA.v17i1.10328

[26] E. P. Patulin, "Scholarship Grants Prediction using Autoregressive Integrated Moving Average (ARIMA) Algorithm," Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 3, pp. 551–555, 2019.
https://doi.org/10.30534/ijatcse/2019/33832019