Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 6, December 2023, pp. 1523-1534
DOI: https://doi.org/10.52436/1.jutif.2023.4.6.1033
p-ISSN: 2723-3863
e-ISSN: 2723-3871

DESIGN OF APPLICATION INFORMATION SECURITY SELF-ASSESSMENT USING VBA AND MSXML2.XMLHTTP CASE STUDY: DISKOMINFO KABUPATEN KAMPAR

Fahmi Rifai[*1], Muhammad Jazman[2], Angraini[3], Megawati[4]

[1,2,3,4]Information Systems Study Program, Faculty of Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia
Email: [1]11950311549@students.uin-suska.ac.id, [2]jazman@uin-suska.ac.id, [3]angraini@uin-suska.ac.id, [4]megawati@uin-suska.ac.id

(Article received: May 7, 2023; Revision: May 16, 2023; published: December 25, 2023)

Abstract

Information security includes the issues that may threaten accountability, reliability, trustworthiness, privacy, authenticity, and trustworthiness of information in an agency. Data and information are very risky things in Information Security, and therefore it is important to do information security governance. The process of evaluating information security using the Index KAMI and ISO 27001: 2013 will be carried out in this study by recording data using Microsoft Excel which has been provided by the National Cyber and Crypto Agency (BSSN). To make it easier to conduct information security assessments and simplify the Excel display, Visual Basic for Applications (VBA) will be utilized as a medium for adding ISO 27001: 2013, then it will be connected using MSXML2.XMLHTTP. The results of the self-assessment carried out show that the Communication, Information, and Signaling Service of Kampar Regency has a level of completeness in implementing the ISO 27001 standard at the "Inadequate" level with a score of 151 only reaching level I+. Meanwhile, the results of the ISO 27001: 2013 Annex control evaluation show that there are still clauses that have not been fulfilled. Therefore, the Communication, Informatics, and Coding Office of Kampar Regency urgently needs improvement in order to fulfill the clauses of ISO 27001: 2013.

Keywords: *Index KAMI, ISO 27001:2013, VBA, MSXML2.XMLHTTP, Information security, self-assessment*

PERANCANGAN APLIKASI KEAMANAN INFORMASI SELF-ASSESSMEN MENGGUNAKAN VBA DAN MSXML2.XMLHTTP (CASE STUDI : DISKOMINFO KABUPATEN KAMPAR)

Abstrak

Keamanan informasi mencakup isu-isu yang dapat mengancam akuntabilitas, keandalan, ketidaktergajaran, privasi, otentikasi dan kepercayaan informasi pada suatu instansi. Data dan Informasi ialah hal sangat berisiko dalam keamanan informasi, oleh karena itu perlu dilakuakan tata kelola keamanan informasi. Proses evaluasi keamanan informasi menggunakan Indeks KAMI dan ISO 27001:2013 akan dilakukan pada penelitian ini dengan perekapan data menggunakan Microsoft Excel yang telah di sediakan oleh Badan Siber dan Sandi Negara (BSSN). Untuk mempermudah melakukan *assessments* keamanan informasi dan menyederhanakan tampilan excel akan dimanfaatkan *Visual Basic for Appliacation* (VBA) sebagai media penambahan ISO 27001:2013, kemudian akan dikoneksikan menggunakan MSXML2.XMLHTTP. Hasil *self-assessment* yang dilakukan menunjukkan Dinas Komunikasi, Informatika, dan Persandian Kabupaten Kampar tingkat kelengkapan penerapan standar ISO 27001 berada pada level “Tidak Layak” dengan skor 151 hanya mencapai tingkat I+. Sedangkan untuk hasil evaluasi kontrol *Annex* ISO 27001:2013 menunjukkan bahwa masih terdapat klausa-klausa yang belum terpenuhi. Oleh karena itu Dinas Komunikasi, Informatika, dan Persandian Kabupaten Kampar sangat membutuhkan perbaikan agar dapat terpenuhinya klausa-klausa ISO 27001:2013.

Kata kunci: Indeks KAMI, ISO 27001:2013, VBA, MSXML2.XMLHTTP, Keamanan informasi, *self-assessment*

1. INTRODUCTION

Security is very important in information technology governance to reduce the occurrence of

threats to assets which include confidentiality, integrity, and availability[1],[2]. Information security aims to reduce business failures, ensure business continuity, and optimize return on investment[3],[4]. Three fundamental components of information security must be maintained: Confidentiality of important information from unauthorized parties. Integration of the information that ensures its accuracy and completeness; and Accessibility of critical services and information for authorized use whenever necessary. This includes issues that may threaten accountability, reliability, trust, privacy, authentication, and confidence in information.[3].

The management of information, especially personal data, is the right and responsibility of public and private data providers and data controllers in managing personal data[5],[6]. If there is an incident of a personal data breach, there will be an investigation of the personal data provider under the Personal Data Protection Bill (RUU PDP). Where in the RUU PDP four important elements discussed which consisted of data owners, data users, data flows, and data security. The existence of the RUU PDP is expected to be able to resolve all problems regarding public data leaks [7],[8].

Data and information are very at risk in the field of information security, therefore it is necessary to carry out information security governance where there are various frameworks that can be used including ISO 27001, ISO 27002, COSO, COBIT, ITIL and others. For now, the most suitable for application in the development of information security processes is SNI ISO / IEC 27001: 2013 [3],[9],[10].

ISO 27001 is a framework for the use of information technology and the management of assets that help organizations ensure that information security is implemented effectively. [11]. The international standard ISO / IEC 27001 is used to define, implement, operate, supervise, review, maintain and improve information security management system (ISMS) policies and documents based on organizational needs. ISO/IEC 27001:2013 defines 14 Main Clauses, and 114 controls[1].

There is a policy that has been established, as information security should be managed. The policy is the Minister of Communication and Information Technology Regulation No 4 of 2016 concerning Information Security Management System[12]. In this regulation, it is stated that two types of guidelines can be used to secure information, namely, the SNI ISO/IEC 27001 standard or the Information Security Index (KAMI) framework prepared by the National Cyber and Crypto Agency (BSSN)[13],[14].

The information security evaluation process uses the US Index and ISO 27001: 2013 with data recording using Microsoft Excel as a tool. To make it easier to assess information security using ISO 27001: 2013 on the Indeks KAMI Excel file that has been provided by the National Cyber and Crypto Agency (BSSN), it will utilize Visual Basic for Applications (VBA) Custom UI as a medium for adding ISO 27001: 2013.

Visual Basic for Application (VBA) is a programming language created by Microsoft and can be used to enhance the capabilities of Office applications, including Ms. Office Excel. By the use of VBA integrated with Microsoft Excel so that data can be recapitulated automatically, then later will be connected using MSXML2.XMLHTTP.

Based on the background described above, this research was carried out by designing the Information Security Self-Assessment application with a case study of the Communication, Informatics, and Coding Office of Kampar Regency using VBA custom UI and MSXML2.XMLHTTP to know the extent of information security readiness and maturity at the Communication, Informatics, and Coding Office of Kampar Regency to get ISO 27001: 2013 Certification and also provide a numerous of recommendations for improving information security management based on ISO 27001: 2013 which can be applied at the Communication, Informatics, and Coding Office of Kampar Regency.

2. RESEARCH METHODOLOGY

This research was conducted at the Communication, Informatics, and Coding Office of Kampar Regency. The subject of research was the Electronic Based Government System (SPBE) and the object of research was self-assessment using the Index KAMI and ISO 27001: 2013 as for the stages of this research can be seen in Figure 1.

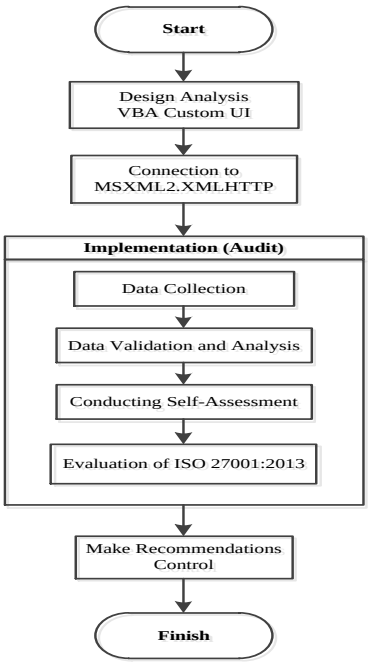

Figure 1 Methodology

The following is an explanation of the research methodology carried out: (1) Performing Analysis and Design of the VBA Ribbon using the Custom UI Editor to simplify the appearance of the KAMI Index Excel and add a ribbon to carry out evaluations using ISO 27001:2013. (2) Making a connection to MSXML2.XMLHTTP which later Excel will be integrated directly into HTTP which can be accessed. (3) Conduct an Information Security Audit in which several stages are carried out at this stage such as data collection in the form of agency risk and asset data, then Data Validation and Analysis carried out to carry out a Checklist which aims to ensure the data provided is following its original state, then conducts a Self-Assessment Information security uses the KAMI Index, then the results of the KAMI Index assessment are then compared with the completeness of the controls in ISO 27001:2013. (4) Make recommendations, after evaluating ISO 27001:2013 it is known that there are deficiencies in the institution so the authors make recommendations based on the completeness of ISO 27001:2013 controls.

2.1. Information Security

Information security is maintaining the confidentiality, integrity, and availability of information[13]. Information security, according to ISO/IEC 27002 (2005), is the Protection of information from any type of threat that aims at ensuring business continuity, risk minimization, and the maximization of return on investment, and business opportunities. [11]. According to the Ministry of Communication and Information Technology (2008), Information security is a branch of information technology study that can be used to determine techniques and methods in protecting information and information systems related to access rights, use, destruction, change, distribution, and destruction without legal authority. The information security types are classified into the following sections: Physical security, Personal security, Operational security, Communication security, and Network security [11].

2.2. Indeks KAMI

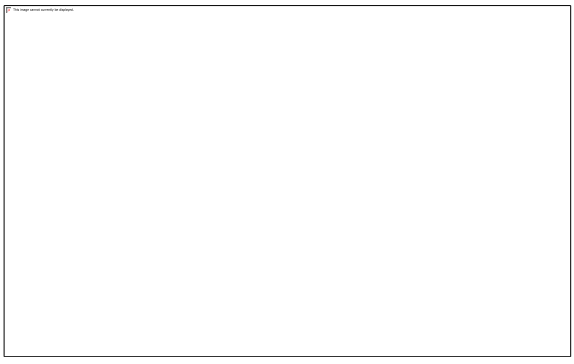

Figure 2 Indeks KAMI

The information security index KAMI is a tool to evaluate and analyze the level of readiness or maturity of the Information Security Management System (ISMS) [15] which will provide the results in the form of a description of the readiness condition (completeness and maturity) of the information security framework to agency leaders then [16]. The Indeks KAMI framework has several parts including electronic system evaluation, governance, risk, framework, asset management, technology, and supplements[17],[18]. In addition, to evaluate the Index KAMI, it can also analyze the similarity with aspects of the guidelines in the SNI ISO 27001: 2013 standard[19],[20].

2.3. SNI ISO/IEC 27001:2013

The International Organization for Standardization(ISO)/*International Electrotechnical Commission*(IEC) 27001 is a framework that provides guidelines for implementing an Information Security Management System (ISMS) [20]–[22] which can be used to make organizational policies, by taking the first step of identifying risks and examining the implementation that has been implemented, and used to determine, implement, operate, supervise, review, maintain and improve information security management system (ISMS) policies and documents based on organizational needs [10],[20],[23].

The ISO 27001: 2013 standard contains clauses that need to be fulfilled to organize a good Information Security Management System (ISMS) [23]. SNI ISO / IEC 27001: 2013 has two parts, namely the PDCA (Plan - Do - Check - Act) section and the Annex Control section. The Control Annex of ISO 27001: 2013 has 14 clauses, security controls, 35 control objectives, and 114 controls for assessment [4],[13]. The correlation between the Index KAMI and ISO 27001: 2013 can be seen in Figure 3, the areas used in the Index KAMI to evaluate or measure the level of control objectives in ISO 27001: 2013 into 5 evaluation areas [24].

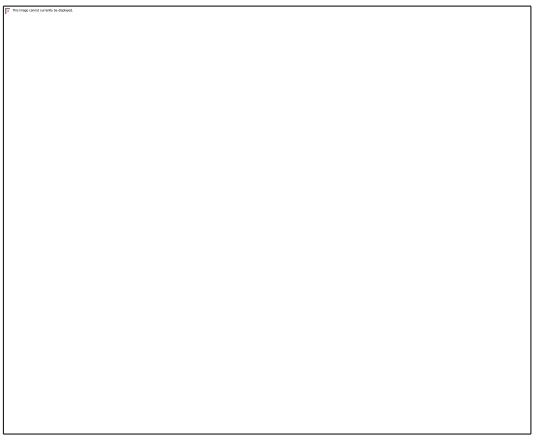

Figure 3 The relationship between ISO 27001 and Indeks KAMI

2.4. *Visual Basic for Applications* (VBA)

Microsoft Visual Basic for Applications (VBA) is a derivative of the Visual Basic programming language developed by Microsoft and released in 1993. VBA is the result of an integrated combination of the programming environment (Visual Basic Editor) with a programming language (Visual Basic) that enables users to design and build Visual Basic programs in the main Microsoft Office application [25], as well as certain applications. VBA is designed to perform several tasks, such as creating alternative specifications of an application such as Microsoft Office or Microsoft Visual Studio [26],[27].

2.5. MSXML2.XMLHTTP

MSXML2.XMLHTTP was first introduced by Microsoft ActiveX in Microsoft Internet Explorer 5 as a control. The way MSXML2.XMLHTTP works to send and receive Hyper Text Transfer Protocol (HTTP) requests that are asynchronous and imprecise. HTTP asynchronously and imprecisely to the Web server, which responds with XML. Responses can be manipulated with scripts from the client or transformed with Extensible Stylesheet Language Transformation (XSLT). MSXML2.XMLHTTP makes it also a possibility to build responsive Web applications that don't need to refresh entire pages to display new data. MSXML2.XMLHTTP works by sending requests to a Web server from a client and returning XML data from the client [28].

3. RESULTS AND DISCUSSIONS

The Office, Communication, Information, and Signage of Kampar Regency have used the Indeks KAMI on electronic systems. The assessment used in index KAMI is an application for analyzing and evaluating the level of readiness (completeness and maturity) of information security implementation and measuring the success of implementation improvement ideas, with the achievement of completeness and maturity levels at the Department of Communication, Informatics and Coding of Kampar Regency.

The list of assets in the Communication, Informatics, and Coding Office of Kampar Regency, where assets are divided into several categories, namely hardware, data, websites, networks, facilities, and human resources. The list of assets at the Communication, Informatics, and Coding Office of Kampar Regency can be seen in Table 1. Meanwhile, risk identification is carried out to find out the threats that might occur later at the Communication, Informatics, and Coding Office of the Kampar Regency. The list of risks at the Communication, Informatics, and Coding Office of Kampar Regency can be seen in Table 2.

Table 1 List of Assets

No	Facilities/Facilities	Amount	Information
1	Building Office	1	Borrow Use
2	Room Work Head Service	1	
3	Room Work Special Secretary/Head of Department	5	
4	Room Work Special Head of Subdivision/Head of Section	1	Not enough 11 room
5	Room Meeting	0	
6	Room BPIM	0	Superimposed in room staff
7	Room Media Center	0	
8	Room servers	0	Superimposed in room staff
9	Vehicle Wheel Four	3	Borrow use
10	Vehicle Wheel Two	0	
11	Computer (PC)	15	
12	Laptops	2	
13	Notebooks	11	
14	Projector	2	
15	Screen Screen	0	
16	Telephone	0	
17	Television	5	
28	Network Internet	320 Mbps	
29	HR	68 People	33 civil servants and 35 non-civil servants

Table 2 List of Risks

No	Asset	Risk
1	hardware	Physical damage to assets
		Full memory
		Virus Attack
2	Data	Data Theft
3	Network	Network Unstable/Network Disconnection

3.1. VBA Ribbon Custom UI Design

VBA is an object-oriented programming language from Microsoft that is mainly used with applications such as Microsoft Excel, Microsoft Word, and Microsoft PowerPoint in nowadays. Microsoft Excel is a data processing application with worksheets in the form of a spreadsheet or worksheet program. The use of VBA in Microsoft Excel is done to add ribbon features. The coding example of making an Excel Ribbon Using the Custom UI Editor is seen in Figure 4.

```
<!-- xml basic bag-i by-ID-->
<customUI xmlns="http://schemas.microsoft.com/office/2009/07/customui">
<commands>
<command idMso="ApplicationOptionsDialog" enabled="true"/>
<command idMso="FileExit" enabled="false"/>
</commands>
<ribbon startFromScratch="true">

<tabs>
<tab id="menu" label="INDEKS KAMI">

<group id="TabGroup1" label=" ">
      <button id="x" label="Kampar" image="kampar" size="large" onAction="diskominfo"/>
</group>

<group id="pp" label=" ">
<button id="AP" image="KAMI1" label="Indeks KAMI Versi 4.0" size="large" onAction="kemi"/>
<button id="TKM" image="notes" label="Catatan Perubahan" size="large" onAction="catatperubahan"/>
</group>

<group id="kemi" label="INDEKS KAMI">
<button id="TK" image="jpg3" label="Tata Kelola" size="large" onAction="tatakelola"/>
<button id="RI" image="risiko" label="Risiko" size="large" onAction="risiko"/>
<button id="KK" image="framework" label="Kerangka Kerja" size="large" onAction="kerangkakerja"/>
<button id="PA" image="Asset" label="Pengelolaan Aset" size="large" onAction="pengelolaanaset"/>
<button id="T" image="TEKNOLOGI1" label="Teknologi" size="large" onAction="teknologi"/>
<button id="S" image="suplemen" label="Suplemen" size="large" onAction="suplemen"/>
</group>
```

Figure 4 VBA Ribbon Coding

The display of the VBA Ribbon coding results is in Figure 5 for the results of the Index KAMI VBA Ribbon design.

Figure 5 VBA Ribbon of Index KAMI

The addition of custom ribbons in the Index KAMI section, namely Index KAMI Version 4.0, Change Record, Risk Security Governance, Asset Management Framework, Technology, Supplements, Respondent Identity, SE Category, and Dashboard. The custom ribbon can be seen in the Figure 6.

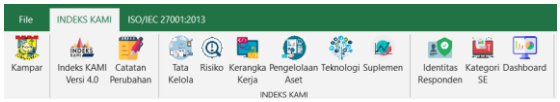

Figure 6 Custom Ribbons in the Index KAMI

Figure 7 for the results of the ISO 27001: 2013 VBA Ribbon design.

Figure 7 VBA Ribbon of ISO 27001:2013

The addition of a custom ribbon in the ISO 27001: 2013 section contains the ISO 27001: 2013 clauses menu and the results of the clause completeness assessment in the form of the Assessment Results menu. The custom ribbon can be seen in the Figure 8.

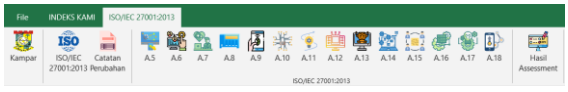

Figure 8 Custom Ribbon in the ISO 27001: 2013

3.2. Applying MSXML2.XMLHTTP

After the custom ribbon is created on the Excel file, a connection will be applied to MSXML2.XMLHTTP. The use of MSXML2.XMLHTTP will perform HTTP Requests in VBA which will provide additional capabilities to Excel. An HTTP request can be used to interact with web services, APIs, or even websites, making it easier for users to access the Excel file. The coding of the HTTP request in Excel VBA can be seen in the figure 9.

```
Sub RefreshFromGithub()

 Dim httpReq As Object
    Dim htmlDoc As Object
    Dim tableObj As Object
    Dim tableRow As Object
    Dim tableCell As Object
    Dim element As Object
    Dim rowNum As Long
    Dim colNum As Long

    Set httpReq = CreateObject("MSXML2.XMLHTTP")
    Set htmlDoc = CreateObject("HTMLFile")

    'Specify the URL from which to retrieve the data
    httpReq.Open "GET    ", "https://fahmirifai.github.io/self-assessment/latest.html", False
    httpReq.send
```

Figure 9 The MSXML2.XMLHTTP coding

3.3. Implementing Self-Assessment and Conformance to ISO 27001:2013 Standards

The data collection process is carried out using observation, interviews, and filling out the Index KAMI questionnaire by correspondents from the Communication, Informatics, and Coding Office of Kampar Regency who have duties and responsibilities based on the areas in the Index KAMI questions, then calculating the results of the questionnaire and analyzing and evaluating the level of completeness and maturity of information security using Index KAMI version 4.0. The results of the analysis are then assessed against the ISO 27001: 2013 Standard. After making a comparison, a recommendation process can be carried out, namely providing input on deficiencies that have not been carried out by the Communication, Informatics, and Coding Office of the Kampar Regency.

A. Evaluation Using the Indeks KAMI

Measurement of 5 information security areas shows the measurement results of parts I, II, III, IV, and V that the maturity level of information security at the Communication, Informatics, and Coding Office of Kampar Regency is at level 1 and 1+, namely Not Feasible. The description of the maturity level of the five areas that have been assessed can be seen in Table 3.

Table 3 Results of Measurement of Maturity Levels in 5 Areas of Information Security

	Governance	Risk Management	Framework	Asset Management	Technology Aspect
		Maturity Level II			
Status	I+	No	No	I+	I+
		Maturity Level III			
validity	No	No	No	No	No
Status	No	No	No	No	No
		Maturity Level IV			
validity	No	No	No	No	No
Status	No	No	No	No	No
		Maturity Level V			
validity	No	No	No	No	No

	Governance	Risk Management	Framework	Asset Management	Technology Aspect
Status	No	No	No	No	No
Final Status	I+	I	I	I+	I+

The order of maturity levels from lowest to highest is I-V. The minimum limit that must be achieved to carry out ISO certification is III +, while for now the maturity level at the Communication, Informatics, and Coding Office of Kampar Regency is only limited to I-I +. The maturity level shows that the position of the Communication, Information, and Coding Office of Kampar Regency is as follows:

- Level I - Initial Conditions
- Level II - Basic Framework Implementation
- Level III - Defined and Consistent
- Level IV - Managed and Measured
- Level V - Optimal

From the description above, it can be seen that the level of maturity at the Communication, Information, and Sign Language Office of Kampar Regency is in the I - I + range, which means it is still in its initial condition. While the Dashboard of the evaluation results of the information security area and the radar chart of the level of completeness of the SNI / IEC 27001 standard can be seen in Figure 10.

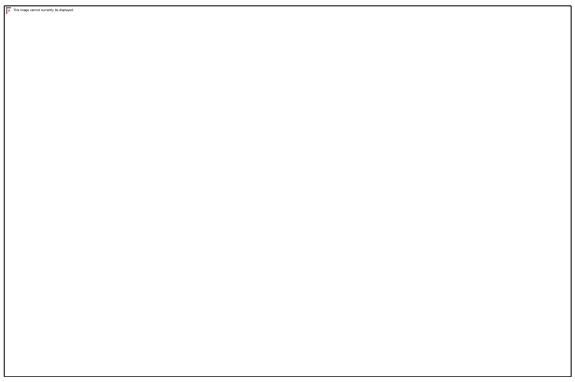

Figure 10 Results of Radar Diagram of the Completeness Level of Information Security Areas

Figure 10 shows that the category level of electronic systems used by the Communication, Informatics, and Coding Office of Kampar Regency is in a high category, with a score of 17. Meanwhile, the level of completeness of the application of the ISO 27001 standard is at the "Inappropriate" level with a score level of 151 only reaching the I + level, this shows that the high level of dependence on Communication, Informatics, and Coding Office of Kampar Regency on electronic systems is not supported by adequate information security. Therefore, based on the results of the evaluation of the Index KAMI, the Communication, Informatics and Coding Office of Kampar Regency is in dire need an improvement.

B. Assessment of Conformance to ISO 27001:2013 Standard

The results of the Indeks KAMI analysis are then assessed for conformity to the ISO 27001: 2013 standard which aims to understand the condition of the information security management system regarding those managed by the Communication, Informatics, and Coding Office of Kampar Regency. The following are the results of the assessment of the suitability of the condition of the information security management system owned by the Communication, Informatics, and Coding Office of Kampar Regency against the ISO 27001: 2013 Standard.

Table 4 Conformance to ISO 27001: 2013 Standard

Area in Standard	Condition	Fulfillment	Conformity Level
A.5 Information Security Policy	2	0	0%
A.6 Information Security Organization	7	5	71%
A.7 Security of Human Resources	6	3	50%
A.8 Asset Management	10	5	50%
A.9 Access Control	14	11	79%
A.10 Cryptography	2	0	0%
A.11 Physical and Environmental Security	15	6	40%
A.12 Operational Security	14	5	36%
A.13 Communication Security	7	3	43%
A.14 System Acquisition, Development and Maintenance	13	2	15%
A.15 Relations with Suppliers	5	1	20%
A.16 Information Security Incident Management	7	2	29%
A.17 Aspects of Information Security in Business Continuity Management	4	1	25%
A.18 Compliance	8	1	13%

Table 4 shows that the results of the assessment using the ISO 27001: 2013 Annex Control show that there are still clauses that have not been fulfilled. Therefore, recommendations will be given in concerning the risk analysis carried out previously, with the recommendations made so that the clauses of ISO 27001: 2013 can be fulfilled to minimize

unacceptable information security risks and improve the quality and ability to manage the Information Security Management System.

3.4. Recommendations

From the results of the evaluation of Indeks KAMI, some values are not sufficient to be certified by SNI ISO / IEC 27001: 2013, therefore researchers will make recommendations for the Communication, Informatics, and Coding Office of Kampar Regency, which in the future, these recommendations will be a reference for making security governance documents to improve information technology security at the Communication, Informatics, and Coding Office of Kampar Regency. The recommendations given are based on the SNI ISO / IEC 27001: 2013 standard, which is carried out by looking at the deficiencies that exist in each area and comparing them with the ISO 27001: 2013 Annex controls relating to that area. The following table presented seberal recommendations from each area sorted according to priority based on the lowest to the highest score obtained for each area.

Table 5 Recommendations for Information Security Governance Areas

No	At the moment	Recommendation	ISO 27001:2013 clause
1	Not yet There is definition standard competence and expertise in implementing information security management	Create competency standard documents/procedures and expertise of SMKI implementers	A.7.2.2
2	There are no applicable requirements/standards related to competency and expertise in implementing information security	Make policies related to competency standards/requirements and expertise of information security implementers	A.7.2.3
3	Information security needs/requirements have not been integrated into the work process	Perform integration related to information security needs	A.7.3.1

Table 5 shows the recommendations given for the information security governance area where ISO 27001: 2013 clauses A.7.2.2, A.7.2.3, and A.7.3.1 are still not fulfilled at the Communication, Informatics and Coding Office of Kampar Regency so that it is necessary to fulfill the clauses in order to achieve ISO 27001: 2013 standardization.

Table 6 Recommendations for Information Security Risk Management Areas

No	At the moment	Recommendation	ISO 27001:2013 clause
1	Not yet set of policies, work programs and deep framework information security	Create documents and framework policies for information security risk management	A.16.1.6 A.8.2.1
2	There is no person in charge of mitigation and supervision of the completion of risk mitigation measures on a regular basis to ensure work progress	Define as well allocate roles and information security responsibility, and make periodic reports so that they can plan for the continuation of mitigation measures	A.16.1.1 A.16.1.2 A.16.1.7 A.16.1.6

Table 6 shows the recommendations given for the Information Security Risk Management Areas where ISO 27001: 2013 clauses A.16.1.6, A.8.2.1, A.16.1.1, A.16.1.2, A.16.1.7, and A.16.1.6 are still not fulfilled at the Communication, Informatics and Coding Office of Kampar Regency so that it is necessary to fulfill the clauses in order to achieve ISO 27001: 2013 standardization.

Table 7 Recommendations for Information Security Management Framework

No	At the moment	Recommendation	ISO 27001:2013 clause
1	Not published yet policy, information security	Advise information security policies	A.5.1.1
2	There is no mechanism for managing information security documents	Create an information security document management policy	A.18.2.2
3	Haven't done yet condition identification which is harmful information security	Do an assessment and decisions about information security incidenti	A.6.1.4
4	Haven't checked yet against audits performed on instance	Make requirements and control activities audits carried out	A.12.7.1
5	Haven't implemented the process yet system development secure (Secure SDLC)	Create policies device development secure software	A.14.2.1
6	Don't have a framework yet management work continuity planning ICT (business	Make a plan security sustainability information	A.17.1.1 A.17.1.2

No	At the moment	Recommendation	ISO 27001:2013 clause
	continuity planning) services		
7	None _ Routine activities For evaluate level obedience security information that already set	Set continuity information security	A.17.1.3

Table 7 shows the recommendations given for the Information Security Management Framework where ISO 27001: 2013 clauses A.5.1.1, A.18.2.2, A.6.1.4, A.12.7.1, A.14.2.1, A.17.1.1, A.17.1.2 and A.17.1.3 are still not fulfilled at the Communication, Informatics and Coding Office of Kampar Regency so that it is necessary to fulfill the clauses in order to achieve ISO 27001: 2013 standardization.

Table 8 Recommendations for Information Asset Management

No	At the moment	Recommendation	ISO 27001:2013 clause
1	The classification of assets has not yet been defined according to the laws and regulations	Create asset documents	A.8.2.1
2	There has been no consistent change in system management	Make consistent management changes to systems, business processes and technology processes	A.12.1.2
3	There isn't any yet regulation security and asset protection relevant agencies RIGHT	Create procedure according to related intellectual property rights	A.18.1.2
4	no storage space designed for disaster risk management	Creating a room equipped with fire detection, temperature and other supporting facilities	A.11.1.4
5	There is no decision yet regarding data exchange with external parties and security	Make a deal regarding the transfer of information	A.13.2.2
6	No regulations yet device security agency computing used outside official work location	Implement security of outside equipment and assets location	A.11.2.6
7	Process not yet available For manage allocations entry key (physical and electronic) to a physical facility	Perform login control	A.11.1.2
8	Process not yet available to check (inspection) And care for: device computers and facilities supporters	Do the process equipment maintenance	A.11.2.4

Table 8 shows the recommendations given for the Information Asset Management where ISO 27001: 2013 clauses A.8.2.1, A.12.1.2, A.18.1.2, A.11.1.4, A.13.2.2, A.11.2.6, A.11.1.2 and A.11.2.4 are still not fulfilled at the Communication, Informatics and Coding Office of Kampar Regency so that it is necessary to fulfill the clauses in order to achieve ISO 27001: 2013 standardization.

Table 9 Recommendations for Information Technology and Security

No	At the moment	Recommendation	ISO 27001:2013 clause
1	no compliance with the implementation of the configuration	access control policy regarding configuration system security must be implemented	A.13.1.1
2	The availability of network infrastructure is not yet available as needed	Perform network infrastructure design as needed	A.17.2.1
3	Network infrastructure, systems and applications are not yet available according to sufficient capacity	Make a network infrastructure design according to the required capacity	A.14.1.1 A.14.1.3
4	Don't have a standard yet For script	Create policies about use cryptographic control	A.10.1.1
5	Haven't implemented yet security for manage encryption keys	Perform management key	A.10.1.2

No	At the moment	Recommendation	ISO 27001:2013 clause
6	System not yet supported password change automatically	Doing management password	A.9.4.3
7	No results recorded yet antivirus updates and virus attack report which was followed up	Execute control against malware	A.12.2.1
8	Every existing application Not yet have specifications and its security function verified/validated	Perform analysis and requirement specifications information security	A.14.1.1
9	B yet to secure development environment and trials	Implement environment safe development	A.14.2.6

Table 9 shows the recommendations given for the Information Technology and Security where ISO 27001: 2013 clauses A.13.1.1, A.17.2.1, A.14.1.1, A.14.1.3, A.10.1.1, A.10.1.2, A.9.4.3, A.12.2.1, A.14.1.1 and A.14.2.6 are still not fulfilled at the Communication, Informatics and Coding Office of Kampar Regency so that it is necessary to fulfill the clauses in order to achieve ISO 27001: 2013 standardization.

4. DISCUSSION

Several studies have evaluated information security using the Index KAMI and ISO 27001: 2013. Based on established policies, information security should be managed. The policy is the Minister of Communication and Information Technology Regulation No. 4 of 2016 concerning Information Security Management Systems. In this regulation, it is stated that two types of guidelines can be used to secure information, namely the SNI ISO/IEC 27001 standard or the Information Security Index (KAMI) framework prepared by the National Cyber and Crypto Agency (BSSN).

The ISO/IEC 27001 international standard is used to define, implement, operate, supervise, review, maintain, and improve, the formation of security management system (SMKI) policies and documents based on the needs of the organization (ISO/IEC 27001, 2013). Assessment using the Information Security Index (Index KAMI) is an application that is used as a tool to analyze, and evaluate the level of readiness (completeness and maturity) of information security implementation and measure the success of implemented improvement ideas, by achieving a certain level of completeness and maturity in an organization.

These studies only focus on evaluating the Index KAMI and then standardizing the fulfillment of ISO 27001: 2013. Where the Index KAMI evaluation tool 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 state of readiness (completeness and maturity) of the information security framework to agency leaders. The Index KAMI can be used to evaluate the level of maturity, the level of completeness of the application of SNI ISO / IEC 27001 as well as a map of information system security governance areas in an agency and a comprehensive standard that assists institutions in achieving goals and generating value through effective information technology governance and management.

In this research, self-assessment is carried out using the Index KAMI and ISO 27001: 2013 to help an organization ensure that the information security implemented is effective so that it can provide recommendations based on the clauses of ISO 27001: 2013. The information security evaluation process uses the Index KAMI and ISO 27001: 2013 with Microsoft Excel data recording. To make it easier to assess information security using ISO 27001: 2013 on the Index KAMI Excel file, it will utilize Visual Basic for Applications (VBA) as a medium for adding ISO 27001: 2013. By using VBA which is integrated with Microsoft Excel so that data can be recapitulated automatically, it will be connected later using MSXML2.XMLHTTP. Meanwhile, previous research did not conduct a Conformity assessment of the ISO 27001: 2013 Standard, design the VBA Ribbon, and connect to MSXML2.XMLHTTP.

5. CONCLUSION

Designing a VBA ribbon using the Custom UI Editor can help Office applications create programs that automate repetitive processes and simplify the appearance of Excel. In addition, the use of MSXML2.XMLHTTP will perform an HTTP Request in VBA that will provide additional capabilities to Excel so that it is easier for users to access the Excel file.

The maturity level of information security at the Department of Communication, Informatics and Cybersecurity of Kampar Regency is at level 1 and 1+, namely Not Feasible with a score level of 151. Therefore, according to the evaluation results of the Index KAMI, the Communication, Informatics and Coding Office of Kampar Regency urgently needs improvement.

The condition of SPBE information security governance managed by the Department of Communication, Informatics and Coding of Kampar Regency is still very far from meeting the requirements of standard ISO 27001: 2013. This is evidenced by compliance which is still far from 100% and a risk profile that has not been mitigated.

The condition of information security governance proves the need for recommendations. Recommendations can be used for the improved quality of information security governance at the Communications, Informatics, and Coding Office of Kampar Regency.

REFERENCES

[1] Candiwan, M. Y. D. Beninda, and Y. Priyadi, "Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division - X Company, In Bandung, Indonesia," *Int. J. Basic Appl. Sci.*, vol. 4, no. 4, pp. 77–88, 2016, doi: 10.13140/RG.2.1.1483.3044.

[2] E. Riana, M. E. S. Sulistyawati, and O. P. Putra, "Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013," *J. Inf. ...*, vol. 4, no. 2, pp. 632–640, 2023, doi: 10.47065/josh.v4i2.2552.

[3] A. F. Manullang, C. Candiwan, and L. D. Harsono, "Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Institusi XYZ," *J. Inf. Eng. Educ. Technol.*, vol. 1, no. 2, p. 73, 2017, doi: 10.26740/jieet.v1n2.p73-82.

[4] A. Saputra and Y. G. Sucahyo, "Rancangan Tata Kelola Organisasi Sistem Manajemen Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten Bekasi," *J. IPTEKKOM J. Ilmu Pengetah. Teknol. Inf.*, vol. 20, no. 1, p. 17, 2018, doi: 10.33164/iptekkom.20.1.2018.17-29.

[5] E. Kavakli, P. Loucopoulos, and Y. Skourtis, "Capability oriented RE for Cybersecurity and Personal Data Protection : Meeting the challenges of SMEs," *IEEE 30th Int. Requir. Eng. Conf. Work.*, 2022, doi: 10.1109/REW56159.2022.00053.

[6] M. Stadnyk and A. Palamar, "Project Management Features In The Cybersecurity Area," *Sci. J. Ternopil Natl. Tech. Univ.*, vol. 2, no. 106, pp. 54–62, 2022.

[7] Yusuf, "Menkominfo: RUU PDP Disahkan, Kominfo Awasi Tata Kelola Data Pribadi PSE," *Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia*, 2022. https://aptika.kominfo.go.id/2022/09/menkominfo-uu-pdp-disahkan-kominfo-awasi-tata-kelola-data-pribadi-pse/

[8] T. A. M. R. Toewoeh, "Teguh : Amanat UU , Presiden Tetapkan Lembaga Otoritas PDP," *Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia*, 2022. aptika.kominfo.go.id/2022/10/teguh-amanat-uu-presiden-tetapkan-lembaga-otoritas-pdp/%0ATitah Arum M. R. Toewoeh October

[9] D. Rutanaji, S. S. Kusumawardani, and W. W. Winarno, "Penggunaan Kerangka Kerja SNI ISO/IEC 27001:2013 Untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI)," *Pros. Semin. Nas. Geotik 2018. ISSN 2580-8796*, pp. 131–140, 2018.

[10] T. J. Mohammed and N. A. Jasim, "Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021)," *Int. J. Health Sci. (Qassim).*, vol. 6, no. April, pp. 10684–10697, 2022, doi: 10.53730/ijhs.v6ns3.8376.

[11] F. A. Basyarahil, H. M. Astuti, and B. C. Hidayanto, "Evaluasi Manajemen Keamanan Informasi pada DPTSI ITS Surabaya," *J. Tek. Its*, vol. 6, no. 1, pp. 122–128, 2017.

[12] KEMKOMINFO, "JDIH KEMKOMINFO," *JDIH KEMKOMINFO*, 2016. https://jdih.kominfo.go.id/produk_hukum/view/id/532/t/peraturan+menteri+komunikasi+dan+informatika+nomor+4+tahun+2016+tanggal+11+april+2016 (accessed Oct. 12, 2022).

[13] H. H. R. H. Ananza, I. Darmawan, and R. Mulyana, "Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2013 (Studi Kasus : Diskominfotik Kabupaten Bandung Barat)," *e-Proceeding Eng.*, vol. 6, no. 2, p. 8368, 2019.

[14] M. Kartika, S. A1, Y. Saintika, and W. A. Prabowo, "Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto," vol. 10, no. 4, pp. 423–428, 2022, doi: 10.26418/justin.v10i4.48977.

[15] A. R. Riswaya, A. Sasongko, and A. Maulana, "Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia)," *J. Comput. Bisnis*, vol. 14, no. 1, pp. 10–18, 2020.

[16] A. Firdani, Suprapto, and A. R. Perdanakusuma, "Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 Menggunakan Indeks Kami Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang," *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 6009–6015, 2019.

[17] Y. D. Wijaya, "Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013," *J. Sist. Inf. dan Inform.*, vol. 4, no. 2, pp. 115–130, 2021, doi: 10.47080/simika.v4i2.1178.

[18] W. Yustanti, R. Bisma, A. Qoiriah, and A. Prihanto, "Analisis Tingkat Kesiapan Dan Kematangan Implementasi ISO 27001:2013 Menggunakan Indeks Keamanan Informasi 3:2015 Pada UPT. PPTI Universitas Negeri Surabaya," *Semin. Nas. PPM Unesa 2018*, no. 4, pp. 1602–1613, 2018.

[19] M. Yunella, A. Dwi Herlambang, W. Hayuhardhika, and N. Putra, "Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 10, pp. 9552–9559, 2019.

[20] A. Hartomo, "Perencanaan Strategis Sistem Informasi dan Sistem Manajemen Keamanan Informasi Bebasis ISO/IEC 27001:2013 Menggunakan Ward & Peppard pada Perusahaan Transshipment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 141–152, 2023, doi: 10.25126/jtiik.2023105604.

[21] Badan Standardisasi Nasional (BSN), "Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan Information technology – Security techniques – Information security management systems – Requirements," 2013.

[22] 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.

[23] N. F. Octariza, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 pada Kantor Pusat PT Jasa Marga," 2019.

[24] P. Sundari and W. Wella, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," *Ultim. InfoSys J. Ilmu Sist. Inf.*, vol. 12, no. 1, pp. 35–42, 2021, doi: 10.31937/si.v12i1.1701.

[25] D. Brkić and Z. Stajić, "Excel vba-based user defined functions for highly precise colebrook's pipe flow friction approximations: A comparative overview," *Facta Univ. Ser. Mech. Eng.*, vol. 19, no. 2, pp. 253–269, 2021, doi: 10.22190/FUME210111044B.

[26] K. W. W. Wong and J. P. Barford, "Teaching Excel VBA as a problem solving tool for chemical engineering core courses," *Educ. Chem. Eng.*, vol. 5, no. 4, pp. e72–e77, 2010, doi: 10.1016/j.ece.2010.07.002.

[27] M. Niazkar, "An Excel VBA-based educational module for bed roughness predictors," *Comput. Appl. Eng. Educ.*, vol. 29, no. 5, pp. 1051–1060, 2021, doi: 10.1002/cae.22358.

[28] A. T. PUTRI, "Sistem Informasi Administrasi Tugas Akhir dan Kerja Praktek Berbasis MSXML2.XMLHTTP (Studi Kasus: Program Studi Sistem Informasi)," UIN Sultan Syarif Kasim Riau, 2018.