# CHAPTER 2

# LITERATURE REVIEW

The importance of information in Indonesia's daily life is expanding dramatically as a result of the rapid development of technology, including the useof technological information in government agencies and public services such as education. To protect data from being used for inappropriate purposes, the Universitas Muhammadiyah Kalimantan Timur (UMKT) stresses the need of securing system technology information. In drafting a security system, technology and information include a variety of topics that should be noted, such as the function of technology, information, and communication, security information management, technology assets, risk, and security information.

## 2.1 Study Related

*Table 2. 1 Study Related*

| No | Writer | Year | Title Study | Method/ Framework Study | Research Results |
|---|---|---|---|---|---|
| 1 | Arif , Sutan Mohammad | 2015 | Kajian Keamanan Teknologi Dan Sistem Informasi Dengan Menggunakan Metode Indeks Kami: Studi Kasus Pada Perusahaan xyz | Indeks Keamanana nInformasi (KAMI) | In study this produce maturity and readiness from framework work security available information previously could said Good / Enough with level moderate ICT dependence in accordance with ISO 27001 standard. |

| | | | | | |
|---|---|---|---|---|---|
| 2 | Muh . Faturachm anHusin , Hans F. Wowor , Stanley DS Karouw | 2017 | Implementasi IndeksKAMI di Universitas Sam Ratulangi | Indeks Keamanana nInformasi (KAMI) | In study this produce obtained score 191 out of 588 score maximum or 32.48%. With this level maturity security information on Sam Ratulangi University still belong to low andneed repair although role / level dependency of ICT is classified asHigh. |
| 3 | Ainun Nafisa ,Faza Hayuhardhi kaiNugrahai Putra, Widhyadma jai Dwi , Herlambang | 2020 | Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur) | SSE-CMM (System Security Engineering-Capability Maturity Model), Failure Mode and Effect Analysis (FMEA), and ISO 2700 Standard | From result analysis obtained by researche rs is still the need repair or enhance ment data security in every related sectors. Like the Review sector Policy, Inventory |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Asset, Control Access, Security Physical and Environment and Security operation. |

In study this there is a number of similarities and differences with study earlier. As for the similarities and differences are:

1. Differences and Similarities Among study this with research conducted by Arif, Sutan Mohammad.

    Study this own similarity with research conducted by Arif, Sutan Mohammad, namely together use method KAMI index. Whereas difference Among both of them located in place research and version Indeks KAMI. The Indeks KAMI used by Arif, Sutan Mohammad is approx 2015 which has version 3.1 while the author use is version 4.1 which version this has been developed more good again so that results obtained later can more detailed and systematic. As for the difference Among versions 3.1 and 4.2 are Revision terms /words in SE Category " Cryptographic techniques specifically certified by the State", Revision the term "Agency" becomes "Company/ Agency", Status Revision "Necessary Repair" to " Fulfillment Framework Basic Work", Revision The condition "Deployment Process" becomes" Application Operations", Addition of Evaluation Area - Party Third, Cloud Services and Personal Data Protection, Dashboard layout changes, revisions and additions Editorial by the BSSN team. Then, the difference next is the place Which research place is researched by Arif, Sutan Mohammad is company xyz whereas Writer do research at UMKT.

2. Differences and Similarities Among study this with research conducted by Muh. Faturachman Husin, Hans F. Wowor, Stanley DS Karouw.

   Study this own similarity with research conducted by Muh. Faturachman Husin, Hans F. Wowor, Stanley DS Karouw that is together use method Indeks KAMI. Whereas difference Among both of them same as difference with previously that is located in place research and version Indeks KAMI. The Indeks KAMI used by Muh. Faturachman Husin, Hans F. Wowor, Stanley DS Karouw around the year 2017 which has version 3.1 while the author use isversion 4.1 which version this has been developed more good againso that results obtained later can more detailed and systematic. Asfor the difference Among versions 3.1 and 4.2 are Revision terms/words in SE Category" Cryptographic techniques specifically certified by the State", Revision the term " Agency " becomes "Company/ Agency", Status Revision" Necessary Repair"to"Fulfillment Framework Basic Work", Revision The condition "Deployment Process" becomes "Application Operations”, Addition of Evaluation Area - Party Third , Cloud Services andPersonal Data Protection, Dashboard layout changes, revisions and additions Editorial by the BSSN team. Then, the difference nextis the place Which research place is researched by Muh. Faturachman Husin, Hans F. Wowor, Stanley DS Karouw is Sam Ratulangi University whereas Writer do research at UMKT.

3. Differences and Similarities Among study this with research conducted by Ainun Nafisa, Faza Hayuhardhikai Nugrahai Putra, Widhy Admajai Dwi, Herlambang.

   Study this own similarity with research conducted by Ainun Nafisa, Faza Hayuhardhikai Nugrahai Putra, Widhy Admajai Dwi, Herlambang that is together do evaluation security data center information. Whereas difference Among both of them same as difference with previously that is located in place research and methods used. The method used by Ainun Nafisa, Faza Hayuhardhikai Nugrahai Putra, Widhy Admajai Dwi, Herlambang are SSE-CMM (System Security Engineering-Capability Maturity

Model), Failure Mode and Effect Analysis (FMEA), and ISO 2700 Standard is Indeks KAMI created by BSSN. Then, the difference next is the place Which research place is Ainun researching Nafisa, Faza Hayuhardhikai Nugrahai Putra, Widhy Admajai Dwi, Herlambang is PT. Pupuk Kalimantan Timur while Writer do research at UMKT.

## 2.2 Evaluation

Evaluation word originated from language English evaluation which contains the basic word "value". The word value or Mark in term evaluation related with belief that something Case that good or bad, right or wrong, strong or weak, enough or not yet enough, and so on. Evaluation could interpreted as a process of considering something Case or symptom with use benchmarks certain character qualitative, for example ok-no good, strong weak, adequate - no adequate, high low, and so on. Evaluation as a process of determining results that have been achieved a number of planned activities for support achievement goal. Evaluation canalso interpreted as activity look for something valuable about something: in search, also includes look for useful information in evaluate existence a program, production, procedure, and proposed alternative strategy for reach goal already determined. (Rukajat. A, 2018)

## 2.3 Draft Security Network

Security network alone often looked at as results from several factors (Ramadhan, 2017) . Factor this varied depending on material basic, but normally at least a number of Case under this included:

1. Confidentiality
2. Integrity
3. Availability

In today's world, computer security is more vital than ever before since it encompasses all aspects of network and computer security. There are others who can enhance the security network computer and merge thethings that might be combined once again with those who are crucial to Case, such as:

1. Nonrepudiation
2. Authenticity
3. Possession
4. Utility
5. Confidentiality

There are several type available information in the a computer network according to (Wajong, 2012). There are a variety of ways in which data may be organized, which necessitates a variety of limits on the use of the data. As a general rule, the information that is accessible to a corporation is private and cannot be shared with other parties. Backdoors, for example, violate business policy since they provide access to the firm's network that the company does not desire. In certain cases, data encryption or the use of a VPN may increase confidentiality. This topic will not be covered in this article, but it will be included regardless. It's common practice to utilize control access to restrict access to a network machine.

It is possible to restrict access to users by using a combination of a username and a password to authenticate people and grant them access. This has been explored and differentiated from context authentication in a variety of environments where work security networks computers are in use.

### 2.3.1 Integrity

Reliable network computer based on facts and data that is currently accessible. Data in transit may be altered by assaults on a network computer, therefore it should not be left unprotected. A "session hijacking" or data manipulation assault known as a "Man-in-the-Middle" may alter the integrity of data transferred between two parties. (Fasihan, B. 2021)

Participants from a "transaction" data must be persuaded that the persons participating in data transmission can be trusted to be dependable and trustworthy in a secure network computer. It is necessary to ensure that the integrity of the data is not compromised throughout the transmission and reception of data at the time of data exchange. A "no" should always signify that "traffic" must be encrypted, but the risk of a "Man in the Middle" attack should not be completely eliminated.

### 2.3.2 Availability

Data or service availability may be checked by the user from a service with ease. if a service (service) is unavailable, it may have a negative influence on a company's productivity and possibly lead to the termination of the manufacturing process. A system's capacity to keep moving and walk with the right requires data availability for all activity networks. (Gani, 2014)

### 2.3.3 Nonrepudiation

In a safe system, everything you do is tracked and recorded, so you canbe sure that the tool you're using to do a system check is doing its job. It is also impossible to separate "log" from the security "system" in the event of an infiltration or other assault. If the cracker is identified and brought to justice, evidence such as "logs" and "notes time," for example, will be crucial. (Badan Kepegawaian dan Pengembangan SDM Daerah Provinsi Bangka Belitung, 2017). For reason this then “nonrepudiation” is considered as a factor important in the security network competent computer. That has defines “nonrepudition ” as following :

1. Ability for prevent a sender for deny then that he has send message or do a action.
2. Protection from denial by one one from entities involved in the a involved communication as well as by whole or part from communication that takes place.

It's important to note that network computers and other data systemsare developed using a wide range of components, each of which has unique security features. If you want to keep your computer secure, you need to be aware of the fact that security is weak in every area of the network. In a chain, the user is a vital link in the process. "Social engineering" is an effective approach to find system weaknesses, and most individuals use "passwords" that can be easily guessed by "social engineering."

To leave the "workstation" unlocked while you eat lunch or do anything else is another meaning of the phrase. Every computer has a system operating system (OS: Windows, Unix, Linux, MacOS), and even routers are powered by a system operating system (SO).

Every system operation has its own unique style and features, and some are even employed for "server" purposes. There are also a variety of issues with system functioning that may be used as a means of stopping system response to the end user.

The "server's" service is an essential part of security. Developers of device security software have announced a fast-closing security hole. Parties who aren't accountable for infiltrating a system or every computer used by its users will take advantage of this vulnerability because of the gap it creates. To keep the problem security "updated," the manager, server, and workstation users must perform regular checks.

As a device with the potential to cause problems with security, it is rather difficult to comprehend. It's not what we believe it is, and if a device hard is installed in an unsafe position, there is a possibility that an unwanted device hard may be installed on the network computer, making penetration much easier. In addition, if an external party has altered the computer network settings, the default configuration will be used.

Additionally, the method of transmission of election results plays an essential part in the security of the issue. Without strong encryption, anybody may intercept "wireless" conversations that are sent over the Internet or other wireless networks. Using a firewall to restrict network computer access is highly recommended. Firewalls may potentially become vulnerable at a single point, allowing a user to feel secure. Because the firewall might become a weakness, data must be allowed to enter and leave network computers that are protected by it. Other than the fact that a firewall can't stop every assault, there are other important points to consider (Badan Kepegawaian dan Pengembangan SDM

Daerah Provinsi Bangka Belitung, 2017).

### 2.3.4 Authenticity

The system should verify that the individuals, objects, and data being exchanged are genuine. Watermarking and digital signatures may be used to confirm the validity of a document, but there are other methods as well, such as tampering detection. (Wahyudiono & Lestiono, 2020).

Common authentication method used is use the username and password. This username/password method there is various type the following types, this is Miscellaneous username/password method:

1. Not there is a username/password

   On system this no username or password is required for access something network. Choice this is the best choice no safe.

2. Static username/password

   On method this is a username/password no changed until replaced by administrator or user. Vulnerable to playback attacks, eavesdropping, theft, and password cracking programs.

3. Expired username/password

   On method this username/password will be no apply until limit time certain (30-60 days) after that should reset, usually by the user. Vulnerable to playback attacks, eavesdropping, theft, and password cracking programs but with level more vulnerability low compared to with a static username/password.

4. One-Time Password (OTP)

   Method this is safest method from all username/password method. Most OTP system based on “secret passphrase”, which is used for create a list of passwords. OTP forces network users for enter a different password every time you log in. A password only used one time. Attack (disruption) against security could categorized as in four category main:

   1. Interruption a asset from something system attacked so that Becomes no available or no could used by the authorities. Example is destruction /

modification to device hard or channel network.

2. Interception a the party who doesn't authorized got access to a asset. The party in question can in the form of people, programs, oranother system. Example is tapping against data in something network.
3. Modification of a the party who doesn't authorized could do change to something asset. Example is change values in the data file, modify the program so that walk with no appropriate, and modify current message transmitted in network.
4. Fabrication a the party who doesn't authorized insert object false to in system. Example is delivery message false to other people.

## 2.4 Data Center

There are several ways to describe data, but the most common is to refer to it as "facts" or "parts of facts." One of the most common topicsin computer-related technology discussions is data. Data has been used ina wide variety of ways.

Etymological definition of Data is the form plural from the Latin DATUM, which meaning "something given." Facts about anything that canbe seen, such as numbers or words, are referred to as "daily data" (Setyawan, 2013). Then Center is English which has a meaning in the middle / centered, which means the Data Center itself is something centered facts in one point with symbols, pictures, values, descriptions a character that has meaning in a context certain.

## 2.5 Data Security

According to (Dinas Komunikasi, Informatika, dan Persandian Kota Bengkulu, 2021) protecting digital information against unauthorized, corrupt, or stolen access is the practice of data security. Concepts here cover everything from device hardware and storage to administrative andaccess control, as well as security logical from application software. It alsocovers the structuring of policies and processes.

How many Type data security:

Data security is there a number of kinds, including Encryption, Firewall, Secure SocketLayer, Cryptography, Pretty Good Privacy.

1. Encryption is a process that does change a code than canunderstand Becomes a code that doesn't can understandable (no readable). Encryption can also interpreted as code or chippers.
2. Firewalls are something security that is as a purposeful filter for prevent (prevent) so that access (to in or to outside) from people who don't authorized no could done.
3. Secure Socket Layer is something shape data encoding so that information confidential as number card credit or control the authentication no could be read or accessed by parties other than owner and server (ownerservice).
4. Cryptography is art encode data. Encode no should means hide although most algorithms developed in theworld of cryptography hu flower with hide data.
5. Pretty Good Privacy is one of the algorithm security datacommunication via the internet for communication daily kind of e-mail. PGP is combined Among system digest creation, encryption symmetrical and asymmetrical.

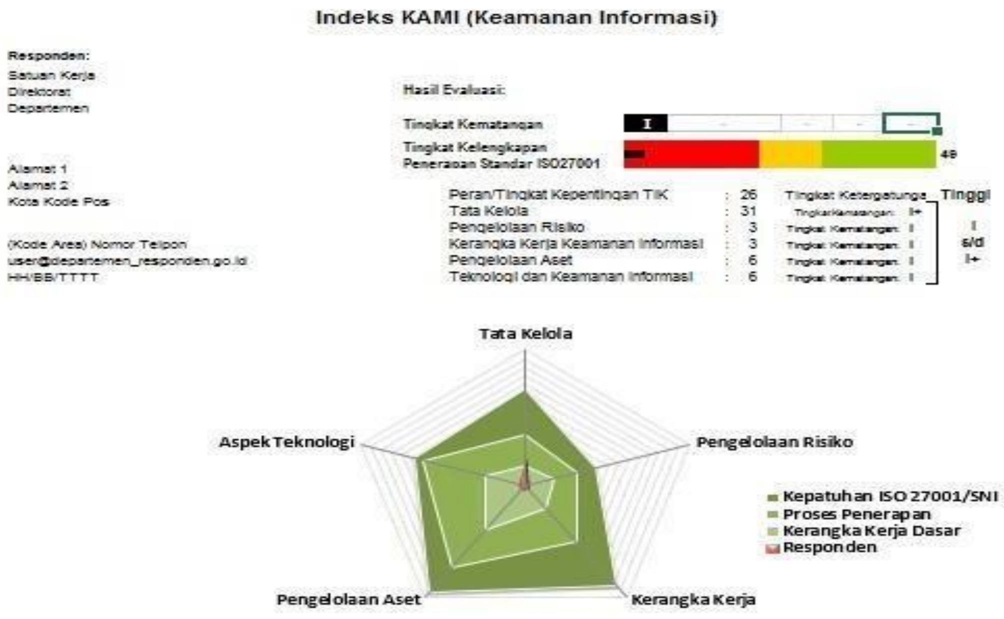
## 2.6 Indeks Keamanan Informasi

According to (State Cyber and Crypto Agency (BSSN), 2019) The Indeks KAMI is a tool for evaluating security preparedness level information in government agencies, as well as a manufacturer and developer of such information. This evaluation framework is not intendedto evaluate the efficacy or suitability of current safeguards, but rather to provide a description of the framework's preparedness (completeness and maturity). Various areas of implementation security information have been evaluated for compliance with the standard SNI ISO/IEC 27001:2013,as well as space for debate.

It was meant to be utilized by government agencies of all sizes andlevels that have an interest in using ICT to aid in the fulfillment of existing tasks and functions, and this is exactly what it does. For example, a description index readiness assessment based on the data used in this evaluation will provide skeletal work security information that can be used and utilized in framework comparisons. Determine the order in which eachstage of the repair or remedy should be completed.

Evaluation could done by periodically in accordance with the needsof each implementing institution. Representative of agency will answer thequestion given in Indeks KAMI with choose the implementation status, namely:

1. Not Done
2. In Planning
3. In Deployment / Partially Applied
4. Applied by thorough



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:

Tingkat Kematangan I

Tingkat Kelengkapan Penerapan Standar ISO27001 49

| | | | | |
|---|---|---|---|---|
| Peran/Tingkat Kepentingan TIK | : | 26 | Tingkat Ketergantunga | Tinggi |
| Tata Kelola | : | 31 | Tingkat Kematangan: | I+ |
| Pengelolaan Risiko | : | 3 | Tingkat Kematangan: | I |
| Kerangka Kerja Keamanan Informasi | : | 3 | Tingkat Kematangan: | I |
| Pengelolaan Aset | : | 6 | Tingkat Kematangan: | I |
| Teknologi dan Keamanan Informasi | : | 6 | Tingkat Kematangan: | I |

I s/d I+

**Figure 2. 1** ***Indeks KAMI Dashboard***

**Source : Badan Siber dan Sandi Negara (2019)**

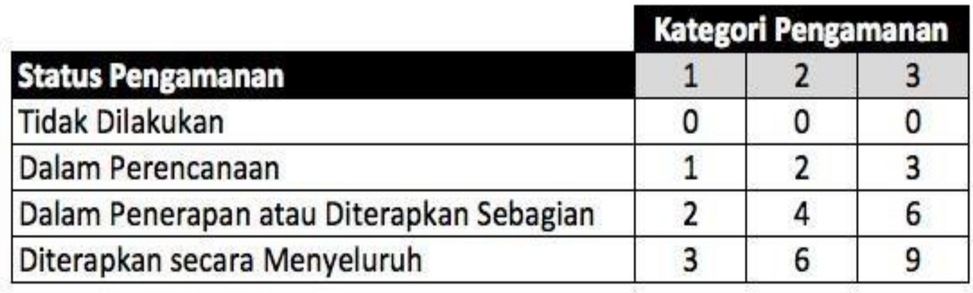
Dashboard Indeks KAMI's representation of the market alone, it hasall the total values of every region in the Indeks KAMI database and uses radar maps and bar charts to display the overall numbers.

Although the use of SNI ISO/IEC 27001 is directed at government agencies, technologies that assist in measuring maturity and completeness in security information (through Indeks KAMI) may also be applied to firmsthat offer service to consumers on large scales.

This work allowed the institution to measure and fix security information so that it might achieve a goal sought by the institution in line with its own demands. A case like this may be possible if the Indeks KAMI were used by repeats:

1. Monitor step improvement or enhancement level management equipment security information.
2. Evaluate governance suitability security after happening significant change in infrastructure or organization existing work in scope evaluation.
3. Ensure implementation of governance security appropriate information.
4. As shape reporting implementation of governance security information to leader.

In this grouping respondents were asked to provide a response ranging from areas related to the form of the basic ICT security framework (questions labeled "1"), the effectiveness and consistency of the implementation of ICT security (labeled "2"), the ability to frequently improve ICT security performance (labeled "3"). The role of ICT in organizations/agencies has a different assessment from several other parts because the role of ICT in these organizations/agencies is expected to get value from the dependence of the organization/institution itself on the role of ICT.



| | Kategori Pengamanan | | |
|---|---|---|---|
| **Status Pengamanan** | 1 | 2 | 3 |
| Tidak Dilakukan | 0 | 0 | 0 |
| Dalam Perencanaan | 1 | 2 | 3 |
| Dalam Penerapan atau Diterapkan Sebagian | 2 | 4 | 6 |
| Diterapkan secara Menyeluruh | 3 | 6 | 9 |

**Figure 2. 2 Score Point of Security Category**

## 2.7 Evaluation Area on Indeks KAMI

The Indeks KAMI helps institution in see and rate level maturity application of SNI ISO/IEC 27001:2013 (Badan Siber dan Sandi Negara, 2019).

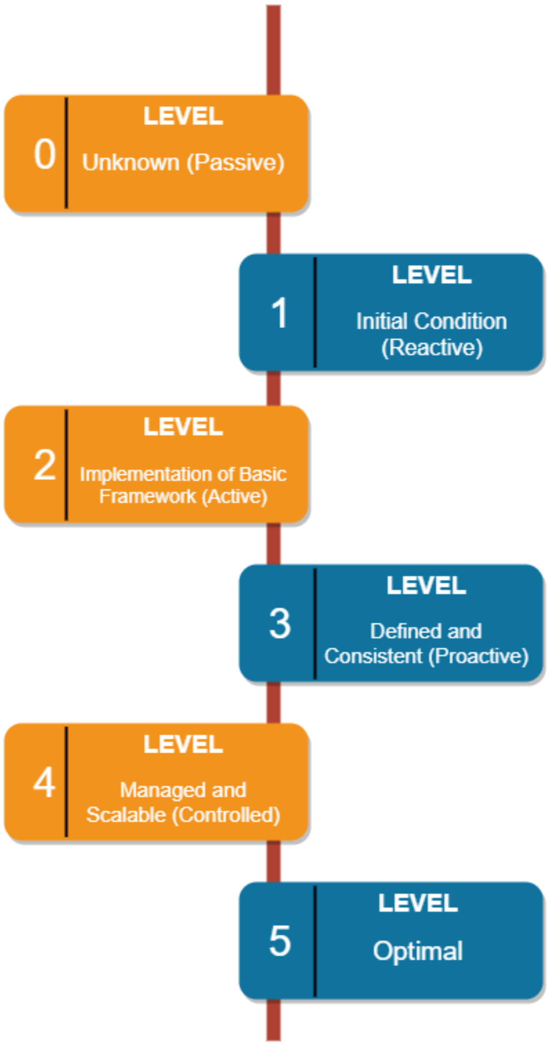

0
LEVEL
Unknown (Passive)
1
LEVEL
Initial Condition (Reactive)
2
LEVEL
Implementation of Basic Framework (Active)
3
LEVEL
Defined and Consistent (Proactive)
4
LEVEL
Managed and Scalable (Controlled)
5
LEVEL
Optimal

**Figure 2. 3** ***Evaluation Areas in the Indeks KAMI***

**Source: Badan Siber dan Sandi Negara (2019)**

The Indeks KAMI evaluates 6 important areas which include:

1. Security Governance Information of this section evaluate readiness governance form security information along with agency / function, duties and responsibilities answer manager security information.
2. Management Security Information of this section evaluate readiness application management risk security information asbase implementation of

security strategy information.

3. Framework Work Management Security Information of thissection evaluate completeness and readiness framework work (policies & procedures) management security information and implementation strategies.
4. Management Asset Information of this section evaluate completeness security to asset information, including whole cycle use asset that.
5. Technology and Security Information of this section evaluate completeness, consistency and effectiveness use technology insecurity asset information.
6. Supplement this Section evaluate for aspect security involvement party third provider service, security service infrastructure cloud (*Cloud Service*) and personal data protection.

## 2.8 Maturity Level Indeks KAMI

Referring of (BSSN, 2019) level Maturityused in Indeks KAMI is divided in 6 levels, namely:

### 2.8.1 Level 0 - No Unknown (Passive)

1. Error status security information no is known.
2. Parties involved no follow or no report rating Indeks KAMI.

### 2.8.2 Level I - Initial Condition (Reactive)

1. Start existence understanding about the need management security information.
2. Application step security still character reactive, no regular, no refers to to whole existing risks, without plot clear communicationand authority as well as without supervision.
3. Weakness technical and non- technical no identified with good.
4. Parties involved no realize not quite enough answer them.

### 2.8.3 Level II - Application Framework Basic Work (Active)

1. Security already applied although part big still in the technical areaand not yet existence linkages step security for get an effective strategy
2. Security process walk without documentation or recording official.

3. Security measures applied operations depend to knowledge and motivation individual executor.
4. Shape security by whole not yet could proved its effectiveness.
5. Weakness in management security still many found and not could solved with completed by the executor nor leader so that causing very impact significant.
6. Management security not yet got priority and not walk by consistent.
7. Parties involved possibility big still not yet understand not quite enough answer them.

### 2.8.4 Level III - Defined and Consistent (Proactive)

1. Shape standard security already applied by consistent and documented by official.
2. Effectiveness security evaluated by periodically, though not yet through a structured process.
3. Party executives and leaders by general could handle problem related management security control with right, will but a number of weakness in system management still found so that could resultin significant impact.
4. Framework work security already obey threshold standard minimum or condition related laws.
5. by general all parties involved realize responsibility they in security information.

### 2.8.5 Level IV - Managed and Measurable (Controlled)

1. Security applied by effective in accordance with managementstrategy risk.
2. Evaluation (measurement) of achievement target safety done by routine, formal and documented.
3. Application security technical by consistent evaluated itseffectiveness.
4. Weakness management security identified with well and consistent follow up improvement.
5. Management security character proactive and implement improvement for reach shape efficient management.

6. Incidents and non -conformity resolved through a formal process with learning root problem.
7. Employee is the part that doesn't inseparable from executor security information.

### 2.8.6 Level V - Optimal (Optimal)

1. Security thorough applied by sustainable and effective through the management program structured risk.
2. Security information and management risk already integrated with Duty tree agency.
3. Security performance evaluated by sustainable, with effectiveness parameter analysis control, study root problems and implementation step for optimization enhancement performance.
4. Security program achievement targets information always monitored, evaluated and improved.
5. Employee by proactive involved in enhancement effectivenesssecurity.