TechHub Journal Vol. 2, No. 1 pp.1-19 (2022)
ISSN: 2810-2800
www.techhubresearch.com

SECURITY ASSESSMENT AND OPEN AND CLOSED SECURITY OPERATIONS AGAINST LOSS IN RED-PLATED COMPANIES

Junaedi

Lecturer of the Department of Government Science, Faculty of Social and Political Sciences, Muhammadiyah University of Makassar

ABSTRACT

Security Assessment and Operation of Closed and Open Security against Losses at the Red-plated Company (PT. Perkebunan Nusantara IV Medan), How to Implement a Security Assessment and Operation of Closed and Open Security Against Losses at the Red-plated Company (PT. Perkebunan Nusantara IV Medan). Analyzing the Implementation of Security Assessment and Operation of Closed and Open Security against Losses at the Red-plated Company (PT. Perkebunan Nusantara IV Medan. To find out the Implementation of Security Assessment and Operation of Closed and Open Security Against Losses at the Red-plated Company (PT. Perkebunan Nusantara IV Medan Regarding losses) resulting from the rampant theft of Fresh Fruit Bunches (FFB) belonging to PT. Perkebunan Nusantara IV or abbreviated as PTPN IV which was allegedly carried out by the surrounding community or controlled by internal employees, which resulted in a decrease in production and also PTPN IV income; PTPN IV macro experienced This very large loss is evident from the decrease in the amount of production which if left unchecked the longer it will get bigger and will cause an endangered situation, so that PTPN IV can have a big name but the result is zero production (extinct) because losses have been found for perpetrators of criminal acts. The crime of theft and embezzlement committed by perpetrators that harmed PTPN IV + 176,000,000,000, - this was based on a letter from the Head of the National Police Security Intelligence Agency No: B/2082/XII/2017/Baintelkam, dated 15/12 2017, regarding: Investigation Results related to Palm Oil Theft at PTPN IV.

Keywords: Security Assessment, Red-Plated Companies, Security Operations

INTRODUCTION

Oil palm plantations play an important role in the national economy and have great potential in national economic development in order to realize the prosperity and welfare of the people in a just manner. Palm oil is still one of Indonesia's mainstay commodities and the largest foreign exchange earner. Based on data from the Indonesian Ministry of Agriculture, palm oil production (palm oil and palm kernel) in 2018 was 48.68 million tons, consisting of: 40.57 million tons of crude palm oil (CPO) and 8.11 million tons Palm Kernel Oil (PKO). The total production came from: smallholder oil palm plantations of 16.8 million tons (35%), large state plantations of 2.49 million tons (5%), and large private plantations of 29.39 million tons (60%) (Ministry of Agriculture Data) RI 2019)

The production of palm oil since 2015 s.d. 2019 in Indonesia can be seen in the table below:

Table 1. Palm Oil Production in Indonesia 2015 – 2019

No	Years	Number of Production (Ton)
1.	2015	31.070.015
2.	2016	31.730.9761
3.	2017	37.965.224
4.	2018	40.567.230
5.	2019	42.869.429

Source: Directorate General of Plantation, Ministry of Agriculture, RI.

Based on the table above, there has been a growth of oil palm that is equal to 19.65%. According to the Indonesian Palm Oil Association (GAPKI), 70% of palm oil production in 2018 was allocated to meet export needs and the remaining 30% for domestic consumption. The value of Indonesia's palm oil foreign exchange contribution throughout 2018 reached USD. 20.54 billion or equivalent to IDR 289 trillion.

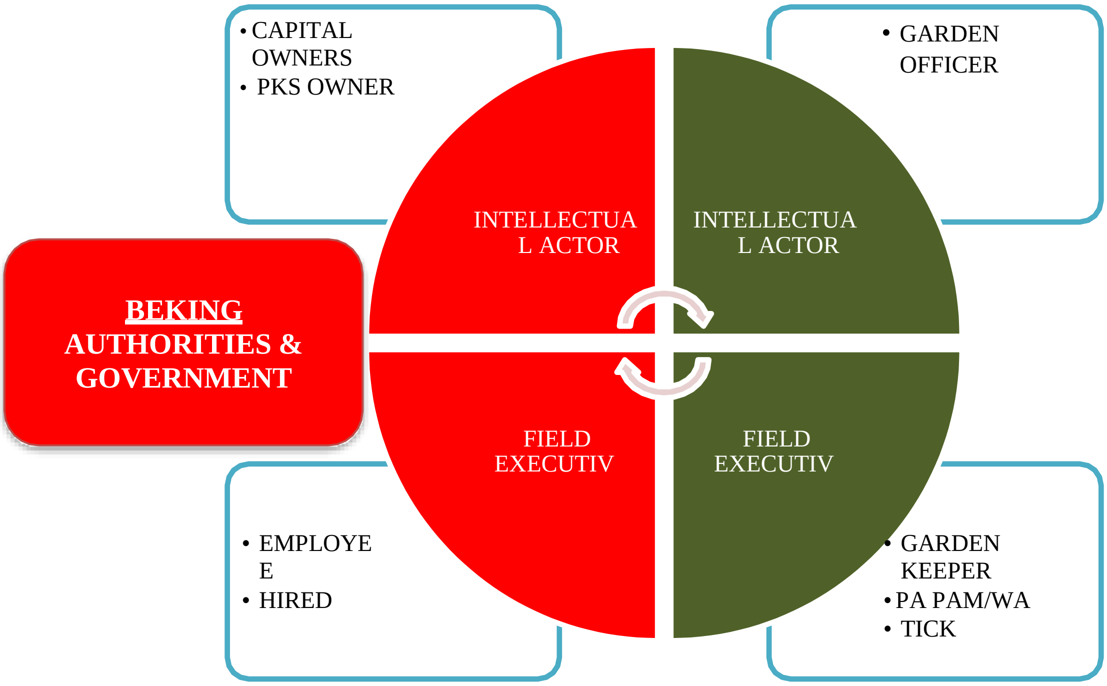
Regarding the losses caused by the widespread theft of Fresh Fruit Bunches (FFB) belonging to PT. Perkebunan Nusantara IV or abbreviated as PTPN IV which is suspected to have been carried out by the surrounding community or controlled by internal employees, which resulted in a decrease in production and also the income of PTPN IV;

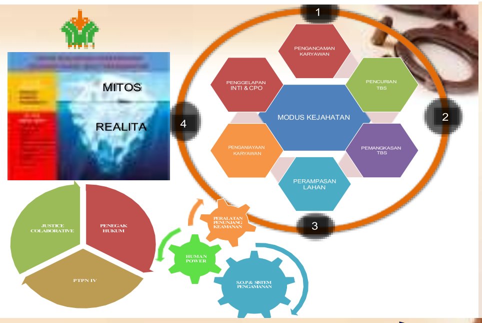
PTPN IV on a macro basis experienced a very large loss, this was evident from the decrease in the amount of production which if left unchecked the longer it would get bigger and would cause an endangered situation, so that PTPN IV could have a big name but the result would be zero production (extinct);

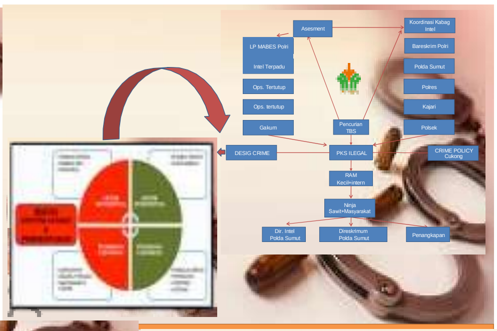
The main purpose of the Assessment I and Assessment II is to assess the magnitude of the theft and who are the main perpetrators of theft, embezzlement and manipulation of FFB in the PTPN IV working area.

In general, the factors that cause the occurrence of these social deviations are (Sikumbang, 2010). (1) "Economic factors are the main cause of social deviations in the community, social problems originating from economic factors are poverty and unemployment; (2) Sociological factors. Social problems originating from sociological factors are problems related to population and other biological imperatives.

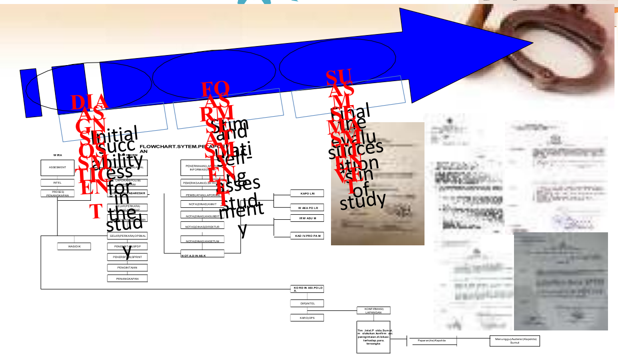
Lack or shaking of these biological factors such as increasing human age and the necessity of fulfilling food needs can encourage people to act socially, including; (a) The factor of having to eat. If a person feels hampered by his desire to meet the need for food, there will be a human effort that leads to social deviations to be able to meet the need for food, meaning that the need for food cannot be postponed; (b) The population factor concerns the uncontrolled increase in the number of people". The purpose of this study was to determine the factors of the Implementation of Security Assessment and Operation of Closed and Open Security against Losses at the Red-plated Company (PT. Perkebunan Nusantara IV Medan) carried out.

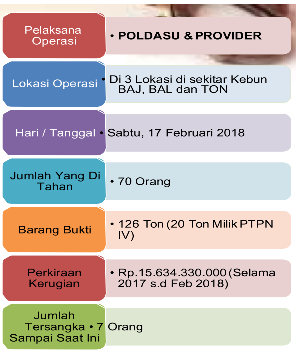






PTPN IV Procedure No. 04.13/Protap/01/X/2018 concerning Integrated Security of PTPN IV Business Unit Assets as an implementation of the Guidelines for Implementing GCG Infrastructure at PTPN IV





Pelaksana Operasi	• POLDASU & PROVIDER
Lokasi Operasi	• Di 3 Lokasi di sekitar Kebun BAJ, BAL dan TON
Hari / Tanggal	• Sabtu, 17 Februari 2018
Jumlah Yang Di Tahan	• 70 Orang
Barang Bukti	• 126 Ton (20 Ton Milik PTPN IV)
Perkiraan Kerugian	• Rp.15.634.330.000 (Selama 2017 s.d Feb 2018)
Jumlah Tersangka Sampai Saat Ini	• 7 Orang

METHODS

The research approach of this article uses a legal analytical descriptive method, which starts from an effort to explain the existing problems through data-based analysis. The data is obtained by taking into account the problems that can arise in the Security Assessment and Operation of Closed and Open Security against Losses at the Red-plated Company (PT. Perkebunan Nusantara IV Medan). The data collected comes from secondary data from the results of research that has been done previously, plus the latest data that has been widely spread in various other supporting literature. Furthermore, the solution to these problems is analyzed as an effort made by the local government, so that it can inspire other local governments to make improvements in services to the community.

RESULTS AND DISCUSSION

The plantation sector is a very important sector and has the potential to be developed in the agrarian sector, so that plantations have an important role (Triningsih, 2016) Based on Article 3 of Law no. 39 of 2014 concerning Plantations (hereinafter referred to as the Plantation Law), states that "Plantation is organized with the aim of; (1) Increase people's income; (2) Increase state revenue; (3) Increasing the State's foreign exchange earnings; (4) Provide employment opportunities; (5) Increase productivity, added value, and competitiveness; (6) Fulfilling consumption needs and domestic industrial raw materials; (7) Optimizing the management of natural resources in a sustainable manner".

PTPN IV as a subsidiary of BUMN which is incorporated as a Limited Liability Company (PT) and is engaged in the oil palm plantation agro-industry has a very important and potential role in contributing to the State in development. Therefore, PTPN IV is expected to be able to contribute to stakeholders for the sake of public welfare.

PT. Perkebunan Nusantara IV as a subsidiary of BUMN (PTPN III Persero) which has total assets as of December 2017 of IDR 14.61 trillion, consisting of: current assets of IDR 1.86 trillion and non-current assets of IDR 12.75 trillion, can not be separated from the legal problems faced. Assets with a total value of more than IDR 14 trillion must be secured for the sustainability and sustainability of the company's business wheels. Securing these assets must start from the smallest, for example in this study is the security of oil palm Fresh Fruit Bunches (FFB) which are often stolen, both by oil palm ninjas, and oil palm mafias. Various modes of crime emerged, such as: FFB theft; FFB pruning; land grabbing; employee abuse; embezzlement of core & Crude Palm Oil (CPO); and employee abuse.

Definition of Security Assessment

Security Assessment is a measurement for a security model on a system in an organization or company (Miles et al., 2004). The security model is the way in which information system security is implemented in an organization (Podungge et al., 2020). This measurement aims to provide information about the information system security gaps that exist in the organization or company which then the measurement results will be used to improve security. Security assessment relies on three interrelated main assessment phases, namely the review phase, the inspection phase, and the testing phase. These three phases can accurately assess the technology, people, and processes that are part of security (Aziz, 2011) as described below.

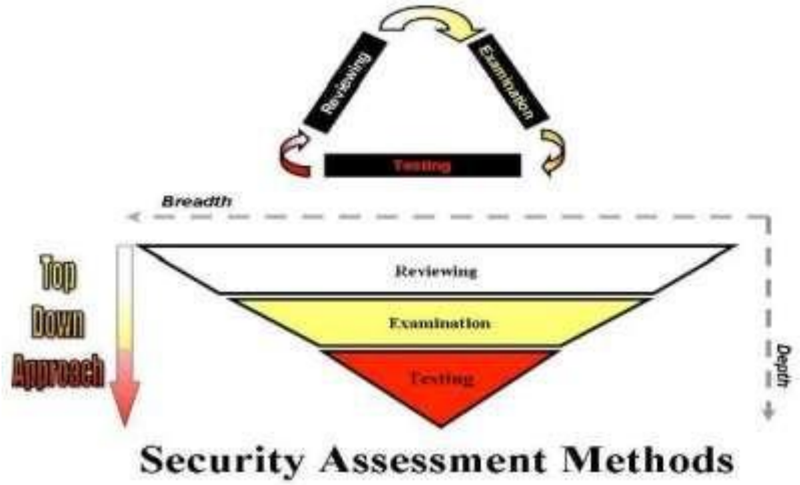


Figure 1. Security Assessment Process (Aziz, 2011)

Review Phase

The review phase is the process of collecting information related to the system that will be carried out in the assessment process. This process can be in the form of interviews with the organization. Information collected includes evaluation of policies, procedures, applications, and networks to find vulnerabilities. This review phase is carried out to understand how the system works.

Inspection Phase

The inspection phase is the process of conducting a technical examination from the system or computer network side to identify security holes in the system. This process includes technical analysis on firewalls, intrusion detection systems, and computer network devices on the system.

Testing Phase

The testing phase, also known as penetration testing, is the process of finding security holes, which allow them to enter a system or network. The review and inspection method will provide useful information for future testing.

Vulnerability Assessment and Penetration Testing

Vulnerability Assessment & Penetration Testing is a method used in conducting a security assessment of an information system. VAPT is a combination of two activities, namely, Vulnerability

Assessment and Penetration Testing. Vulnerability Assessment is a process of scanning systems, software, or computer networks to find weaknesses or loopholes in the system. This weakness can be in the form of a backdoor that can be used to attack the system (Goel & Mehtre, 2015).

Penetration Testing is the next stage of vulnerability assessment. Penetration Testing is the stage of exploitation of the system carried out in a legal way to find security holes that may be exploited in the system. At this stage the tester has the right to try to enter the system and exploit it (Goel & Mehtre, 2015).

Nessus

Nessus is one of the most widely used security vulnerability assessment products first released by Renaud Deraison in 1998. It has become one of the most popular vulnerability scanning tools used across the industry for the last 15 years (Kumar, 2014). Nessus provides vulnerability scanning for network devices, virtual hosts, operating systems, databases, web applications, and IPv4/IPv6 hybrid networks (Li, Liang, Yang, & Chen, 2010). Nessus uses Common Vulnerability and Exposure (CVE) as its standard. CVE is a standard for naming information security vulnerabilities. Nessus uses Common Vulnerability and Exposure (CVE) as its standard. CVE is a standard for naming information security vulnerabilities (Li et al., 2010). One of the interesting features of Nessus is that it is an open source application and many people are contributing every day. There will be plug-ins for new vulnerabilities within days after the security vulnerabilities are released to the public (Mukhopadhyay et al., 2014).

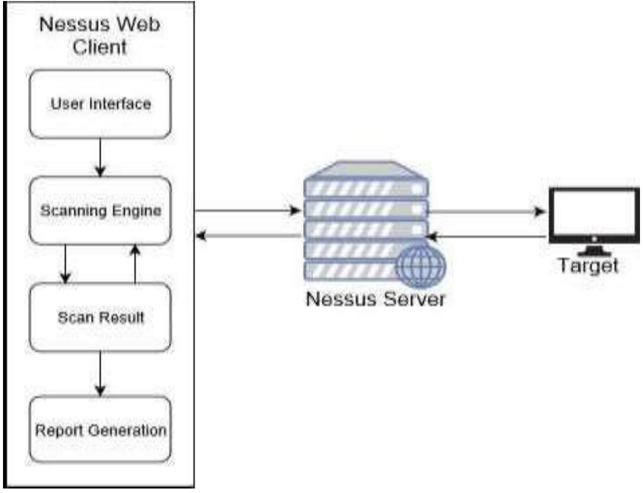


Figure 2. Nessus Scanner Work Flow

The NIST Cyber Security Framework is a process for identifying, assessing, and responding to an ongoing risk. In managing a risk, the organization must understand the likelihood of an event occurring and the potential impact. With this information, organizations can determine the level of risk they may face (National Institute of Standards and Technology, 2018).

Information Security Management ISO 27001:2013 is a security standard that focuses on safeguarding information used to secure data, which outlines the recommended requirements for establishing, monitoring, providing organizational guidance on how to create, implement and maintain and improve an information security management system (ISMS). ISO 27001 has a standard that focuses on maintaining the confidentiality of customer and stakeholder information and maintaining its integrity, aiming at emphasizing the identification, evaluation and management of risks that can be accepted by information systems (Davis et al., 2016).

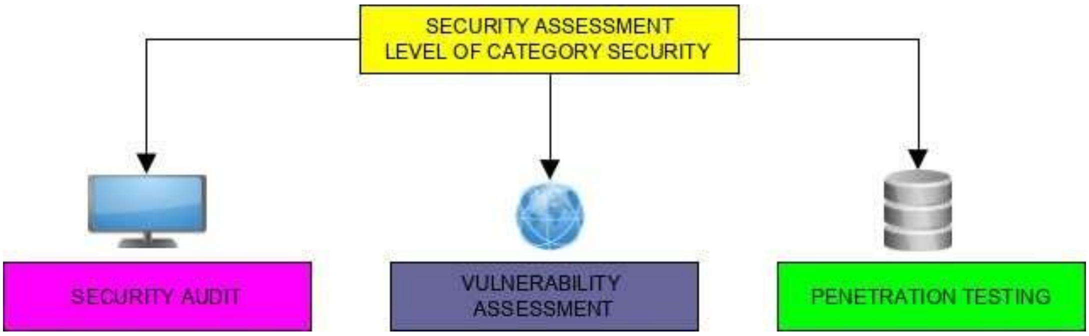
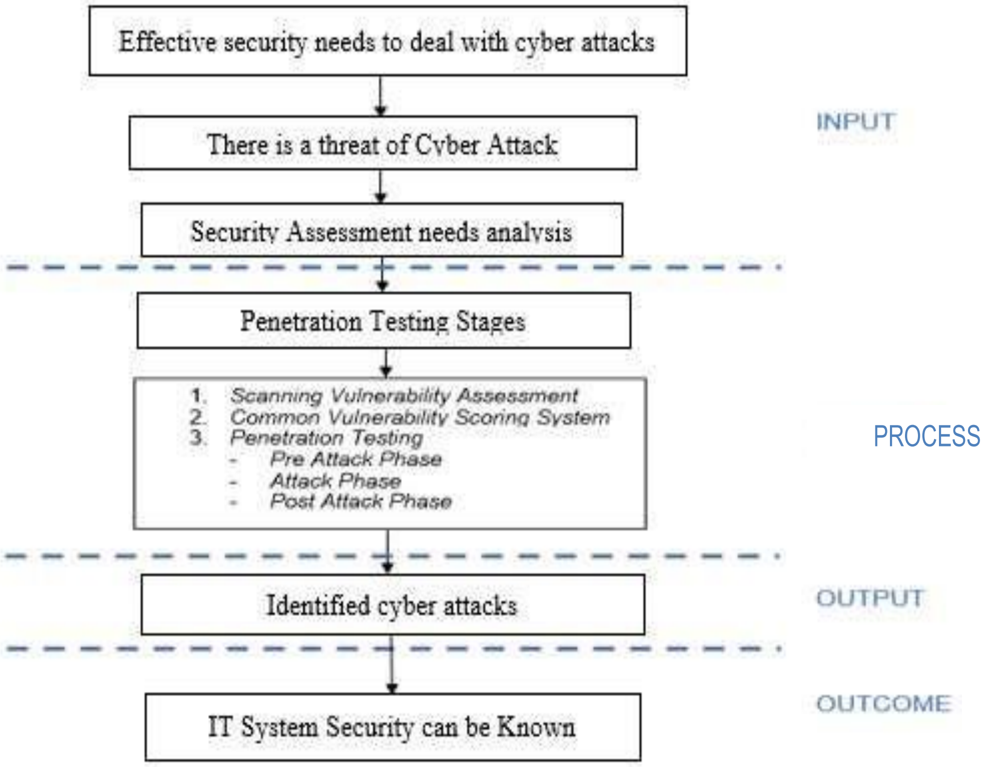


Figure 3. Security Assessment Category Level Source: Critical Ethical Hacking, 2012

Six Ware Network Security Framework is an initial security framework concept, comprehensive network security as a solution to improve an organization's network security resilience from threats, attacks and vulnerabilities, this method is an operational level security strategy that allows to find out the most efficient and effective actions which can provide solutions in network security (Gultom et al., 2018), Open Web Application Security Project (OWASP) Framework (detailed explanation is attached in the next chapter) in this case the researcher focuses on assessing web server security through penetration testing methods, the right framework and in conducting this research, OWASP has the largest data system security method ever collected in the preparation of application security standards. This framework is used as an application security standard in conducting vulnerability assessments using the standard open web application security project framework in addressing the most impactful application security risks currently facing an agency (Disterer, 2013).

Penetration testing is an important step in the development of a secure server computer-based defense system that is connected in a network in any case because it not only emphasizes the operation, but the implementation and design of the system. it is an official and scheduled action that separates penetration testers from attackers and has been widely adopted by organizations and institutions.


Effective security needs to deal with cyber attacks
There is a threat of Cyber Attack
Security Assessment needs analysis
INPUT
Penetration Testing Stages
1. Scanning Vulnerability Assessment
2. Common Vulnerability Scoring System
3. Penetration Testing
- Pre Attack Phase
- Attack Phase
- Post Attack Phase
PROCESS
Identified cyber attacks
OUTPUT
IT System Security can be Known
OUTCOME

Open Web Application Security Project (OWASP) Framework (detailed explanations are attached in the next chapter) in this case the researcher focuses on assessing web server security through penetration testing methods, the right framework and in conducting this research, OWASP has the largest data system security method ever. collected in the preparation of application security standards. This framework is used as an application security standard in conducting vulnerability assessments using the standard open web application security project framework in dealing with the most impactful application security risks currently facing an agency (Shrestha, 2012)

Penetration testing is an important step in the development of a secure server computer-based defense system that is connected in a network in any case because it not only emphasizes the operation, but the implementation and design of the system. it is an official and scheduled action that separates penetration testers from attackers and has been widely adopted by organizations and institutions (Yunanri et al, 2016). In addition, penetration testing is used as an evaluation of security on computer systems or network servers by identifying weaknesses (vulnerability) as identification in the form of security holes, configurations, firewalls and wireless points (OWASP Zed Attack Proxy Project, 2019).

The steps in the vulnerability assessment include vulnerabilities collected from several ministries and cyber agencies in Indonesia. In the vulnerability assessment, the stages that will be passed are through the Scanning SQL Injection stage, namely looking at weaknesses through databases such as SQL, XAMPP, Broken Authentication looking at weaknesses in passwords and usernames, Sensitive Data Exposure looking at weaknesses in sensitive data such as weaknesses in encryption that cause data and identity theft. XML External Entities (XEE) view untrusted data sources in XML documents, Broken Access Control allows attackers to bypass the authorization process and can do things an admin would normally access.

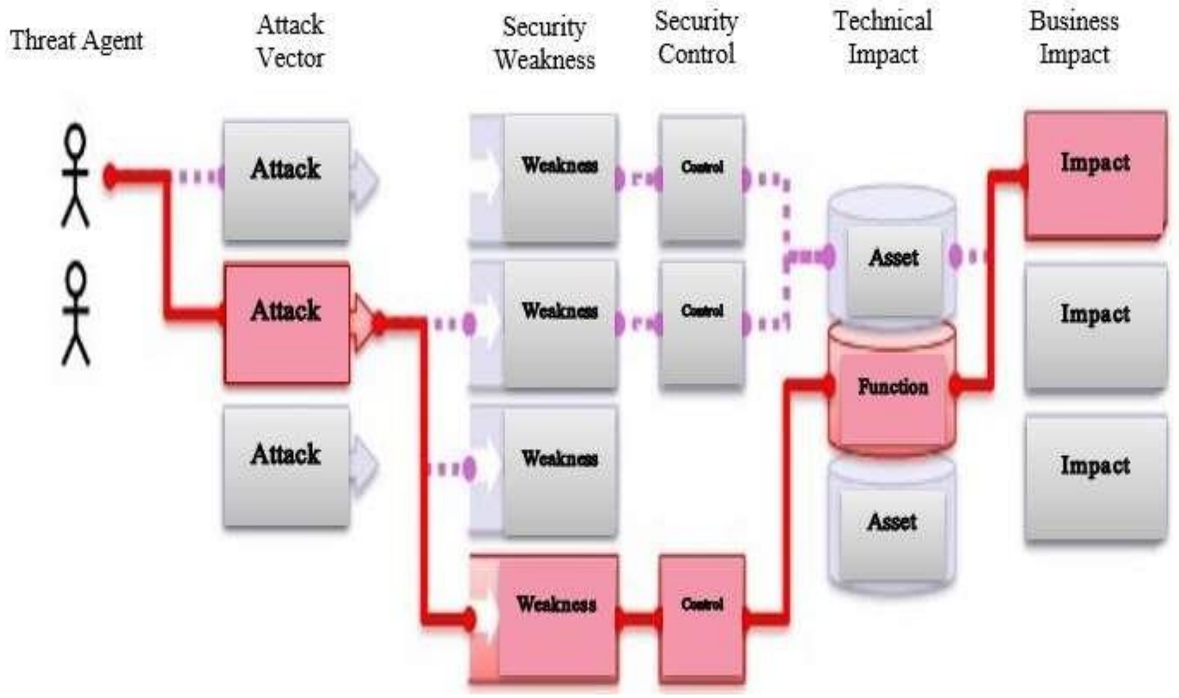


Figure 4. Scanning Vulnerability Stages Source: OWASP, 2017

Security Assessment

Information Systems Security Assessment Framework (ISSAF). is a structured framework from the Open Information System Security Group that groups information system security assessments into several domains and assesses specific details or testing criteria for each domain.

The Open Web Application Security Project (OWASP) is a free and open worldwide community focused on improving the security of application software. OWASP's mission is to make application security "visible", so that people and organizations can make informed decisions about application security risks. The results of this OWASP test will be mapped using the Risk Rating assessment parameter. Risk Rating is an assessment parameter used to measure the level of a risk. In this methodology, risk is the product of likelihood (Likelihood) and impact (Impact).

Assessment Flow

The security plan is very important, because it is the basis for developing a business continuity plan, which contains steps and procedures to always maintain business continuity that may be disrupted by disruptions that may occur.

In the Information Security Plan Template, issued by the OTDA, information security contains other concepts, namely risk management, policies, procedures, standards, guidelines, information classification. , security operations and security awareness.

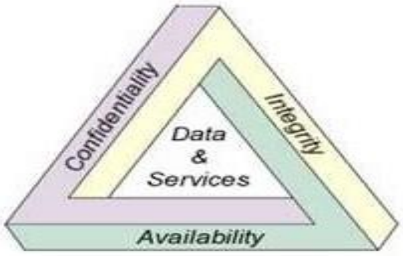


Figure 5. CIA triangle

In accordance with Figure 1, there are important principles of an information security plan, namely: confidentiality, data integrity and availability. CIA is a standard used by many to measure the security of a system. The principles of information security are as follows; (1) Confidentiality, namely limiting access to information only for certain users; (2) Integrity of data/information (integrity), namely the level of trust in an information. This concept includes data integrity and source integrity; (3) Availability, namely availability, is absolutely correct. Availability in question is the availability of information sources.

A security plan must be able to combine the roles of policy, technology and people, where humans (people), who run the process need policy support (policy), as a guide to do so, and require technology as tools

A security plan, must be able to describe systematic steps to reduce risk, by implementing security controls based on their objectives. Types of control based on the target, as follows; (1) Administrative control (administrative security); (2) logical control, intrusion detection, and anti-virus; (3) Physical control.

Security controls are inseparable from the protection of sensitive information assets. Enterprise Information Technology Services (2001), in his article entitled “Information Classification Standard”, explains that information is classified into sensitive and critical information. Sensitive information is related to confidentiality and data integrity (integrity), while critical information is related to data availability.

Based on the description above, the security plan will contain the determination of the combination of information security controls used, as well as priorities in carrying out their implementation. The basic contents/contents of the information security plan document, among others; (1) Threats and weaknesses, is a process to review the results of the risk assessment stage, by taking information about something that can disrupt the organization's activities; (2) Goals and targets, is the process of determining the targets and scope of information security to be achieved, so that they can focus on the security aspects that will be resolved. Information security objectives describe specific outcomes, events or benefits to be achieved in accordance with the established security objectives; (3) Rules and responsibilities, is the process of formulating rules and responsibilities, which regulate activities in an effort to reduce information security risks that originate from threats and weaknesses; (4) Security strategy and control, is a process to prioritize actions to be taken to achieve the stated information security goals and objectives. The priority of these actions is as a safeguard to maintain the confidentiality, integrity and availability of information, by determining security controls that are in accordance with the desired goals and objectives.

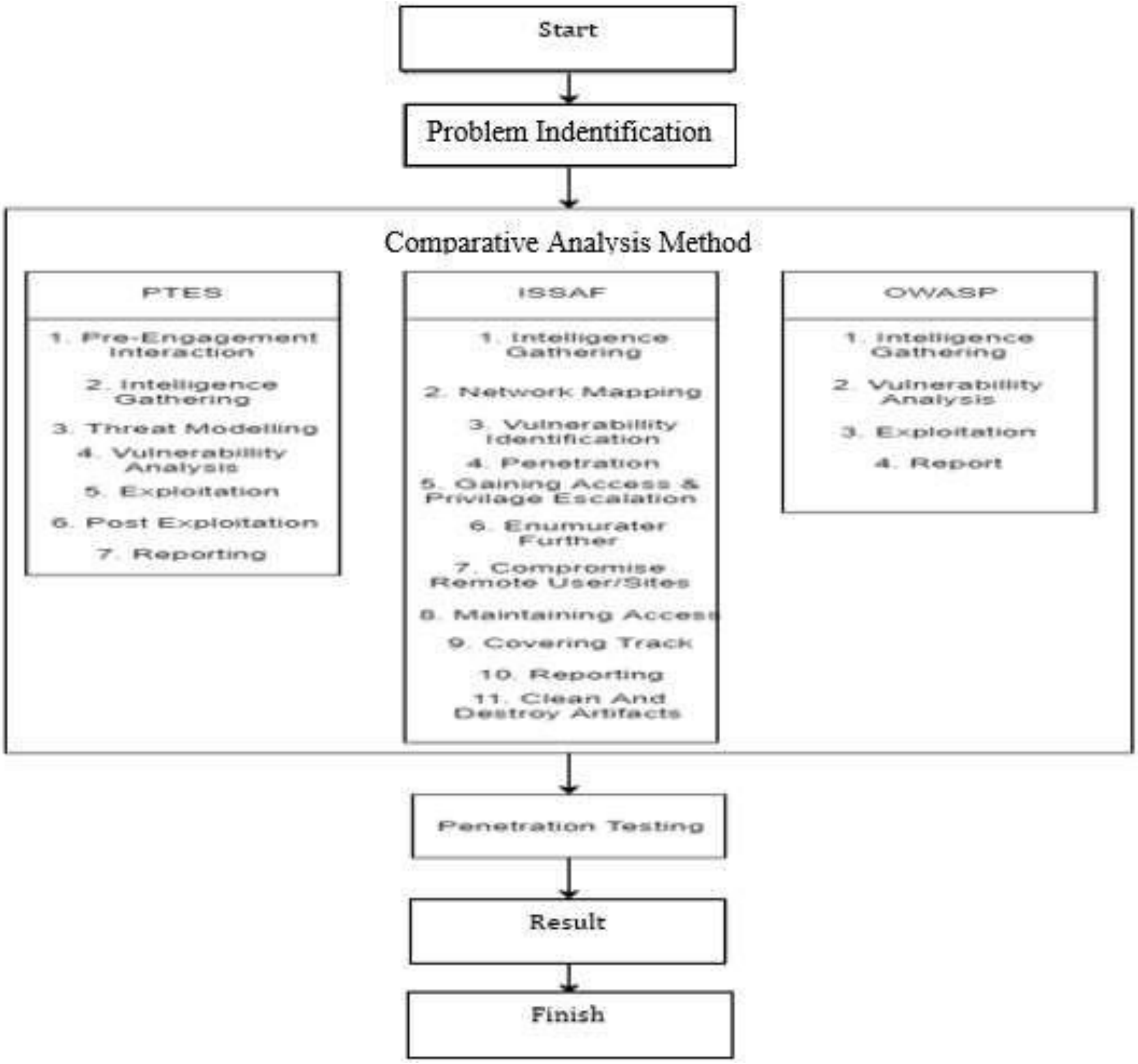
Risk Analysis Results

The risk analysis will ultimately provide the results of risk identification, along with recommendations for security controls related to efforts to reduce these risks. This stage is called the control recommendation.

Control recommendations will be the result of the risk assessment process and will become inputs for the risk mitigation process, as well as recommendations for procedures and techniques in information security planning that will be implemented in the future.

The recommendations resulting from or risk analysis are as follows; (1) Risks that are categorized at the "Low" level, with a rating of 1 to 5, are of low risk value, so that they are acceptable; (2) Risks categorized at the "Medium" level, with a rating of 6 to 10 of medium value, with a recommendation that the risk is unacceptable, so that the risk must be eliminated, reduced or transferred; (3) Risks categorized at the "High" level, with a rating of 12 to 16 are of high value, with a recommendation that the risk is unacceptable, so that risk must be eliminated, reduced or transferred.

The risk of the company's business stopping, because it does not have a disaster management plan, so that when a disaster occurs it is not able to maintain security support for the running of the business, systematically.


Start
Problem Indentification
Comparative Analysis Method
PTES
1. Pre-Engagement Interaction
2. Intelligence Gathering
3. Threat Modelling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting
ISSAF
1. Intelligence Gathering
2. Network Mapping
3. Vulnerability Identification
4. Penetration
5. Gaining Access & Privilage Escalation
6. Enumurater Further
7. Compromise Remote User/Sites
8. Maintaining Access
9. Covering Track
10. Reporting
11. Clean And Destroy Artifacts
OWASP
1. Intelligence Gathering
2. Vulnerability Analysis
3. Exploitation
4. Report
Penetration Testing
Result
Finish

Threats and Vulnerabilities

Threats and vulnerabilities/weaknesses can describe the risks that are potentially accepted by the company, based on the assets owned by the Plantation Company which are assessed at the risk assessment stage, information on vulnerabilities/weaknesses and threats can be generated.

According to Mell & Grance (2002) in the NIST Standard compatibility means that the recommended control must be in accordance with the identified vulnerabilities, which will be eliminated or reduced. Meanwhile, the effectiveness of the recommended security control depends on its ability to reduce the risk or impact caused by vulnerabilities/weaknesses, so that the level of protection against assets owned by the company can be known.

Rules and Responsibilities

Information security is not only related to technical issues, but also must be supported by the rules and responsibilities issued by the organization, in the form of information security governance.

Conner & Coviello, (2004) explains that information security governance is one part of the concept of good organizational governance, which consists of a set of policies and internal controls of the company that are coordinated and managed.

In the concept of information security governance, it is conveyed that there is a set of responsibilities and functional rules. The collection of responsibilities on information security in the company, as follows; (1) Responsible for managing the overall operation of the company's information security; (2) Responsible for making reports and explanations to consumers and the public; (3) Responsible for designing security policies, procedures, programs and information security training; (4) Responsible for responding to information security incidents/incidents by conducting investigations, mitigation, and prosecutions; (5) Responsible for responding to audit reports regarding information security; (6) Responsible for conducting audits, conformity and needs assessments of security controls; (7) Responsible for communicating and disseminating policies, programs and training to all employees related to information security; (8) Responsible for implementing and implementing all information security policies, procedures and programs, as well as reporting if security vulnerabilities/weaknesses are found.

The functional rules on information security governance are; (1) Chief Executive Officer (CEO); (2) Chief Security Officer (CSO), or Chief Information Officer (CIO), or Chief Risk Officer (CRO), or Department/Agency Head (DH); (3) Mid-Level manager: (4) Staff or employees

Based on the set of responsibilities and functional rules, they can be grouped as shown in the figure below:

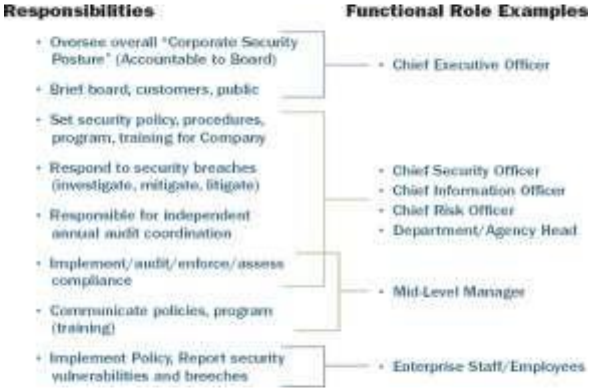

Responsibilities
Functional Role Examples
Oversee overall "Corporate Security Posture" (Accountable to Board)
Brief board, customers, public
Chief Executive Officer
Set security policy, procedures, program, training for Company
Respond to security breaches (investigate, mitigate, litigate)
Responsible for independent annual audit coordination
Chief Security Officer
Chief Information Officer
Chief Risk Officer
Department/Agency Head
Implement/audit/enforce/assess compliance
Communicate policies, program (training)
Mid-Level Manager
Implement Policy, Report security vulnerabilities and breeches
Enterprise Staff/Employees

Figure 6. Image Responsibilities and functional rules

Responsibilities and functional rules are closely related to the organizational structure that applies in the organization, so it is necessary to display recommendations on organizational structure on corporate information security governance, as in the picture the two organizational structures recommended by the concept of information security governance, then need to conduct an analysis of organizational structure of the company

The company's organizational structure places the Divisions related to IS and IT management at the third level from the top management, so that decision-making and giving considerations in setting policies do not have a big influence.

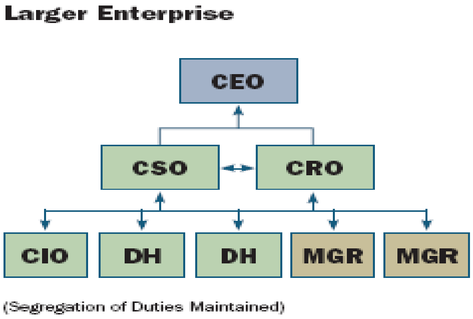


Figure 7. Recommendation of Information Security Organizational Structure (Larger)

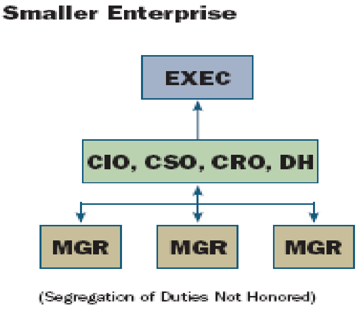


Figure 8. Information Security Organizational Structure Recommendation (Smaller)

Based on the above considerations, it is recommended to gradually change the company's organizational structure, which leads to good IT governance and good information security governance, all of which refer to the big concept, namely governance. good corporate governance (good corporate governance).

Security Assessment Results

Goals

The purpose of corporate security is to increase the ability to prevent, protect, respond and return to a safe condition from security breaches. Strategic objectives are specific things to help achieve the objectives of information security set out in a securityplan.

Success in achieving goals will be determined by the goals that can be met. The explanation of each goal is discussed in the next section.

The first objective of the information security plan is to determine the policies needed to support the implementation of information security. If the target can be achieved, it will provide benefits to the company in maintaining the security of its information. The expected benefits of achieving this target are as follows; (1) Policies and procedures for classifying plantation security information; (2) Garden security policies and procedures; (3) Policies and Procedures for recording incidents of security disturbances; (4) Garden security error correction procedure; (5) Policy on integration of garden security application systems; (6) Policies to measure the performance and burden of the garden security system; (7) firewall policy on the local network security garden; (8) Maintenance procedures for garden security supporting devices; (9) Garden safety prevention policies and procedures; (10) Procedure for data backup and garden security system.

The second target is to identify the needs of Human Resources (HR). The third target is to identify the system development and maintenance from the information security aspect. The fourth target is to be able to identify critical company assets belonging to the company, as well as identify risks, threats and vulnerabilities. The fifth goal is to identify potential information security incidents. The sixth goal is to identify the physical management and information security environment. The seventh goal is to identify the management of communications and information security operations. The eighth goal is to be able to conduct an audit and then correct any errors or disturbances that occur.

Strategy

The security strategy for oil palm plantations is an important part of a comprehensive plan for the security of oil palm plantations from criminal acts of theft, land grabbing. In each of these strategies, a collection of actions that need to be taken in the implementation of the strategy will be presented, in an effort to achieve the goals and objectives that have been determined. The first strategy is to develop policies, procedures and standards related to oil palm security. This strategy is carried out by identifying important policies, procedures and standards to be formulated and established, where the second strategy is to improve the recruitment and training pattern of the security team. This strategy is carried out by conducting background checks on the prospective security team.

The third strategy is to implement preventive and detection tools against attacks and security disturbances in Oil Palm Plantations. This strategy is carried out by scanning the Oil Palm Plantation.

The fourth strategy is to apply a pattern of inspection and evaluation of the security of Oil Palm Gardens for information security. This strategy is carried out by increasing supervision activities on the work of a large number of operators, so that authentication and authority are managed.

Security Control

The objectives of the security plan can be achieved if the predetermined objectives have been met. Furthermore, each target can only be achieved if implementing several information security strategies, and each strategy provides recommendations for actions that must be taken, in an effort to achieve the predetermined goals.

As for the security controls, Security strategies and controls are obtained based on the results of the risk assessment and mitigation process. The risk assessment produces risk levels and recommendations for security controls, based on an assessment carried out on eight aspects, namely; (1) Management of Oil Palm Plantation security policy; (2) Management of company assets; (3) Management of security human resources; (4) Physical management and security environment; (5) Management of security operations; (6) Management of system development and maintenance.

The risk collection and its levels are then used as the basis for recommending security controls that can prevent or reduce these risks, so that the risk assessment process will produce several things, namely; (1) Risks derived from weaknesses/vulnerabilities and threats to critical assets owned by the company; (2) The value of the risk obtained from the trend and the impact that can be caused by the risk if it occurs; (3) Recommendations for information security controls, based on the risks being mitigated.

The stages of risk mitigation have resulted in several things, namely; (1) Priority of action to be taken in order to mitigate risk; (2) The results of the evaluation of the recommended safety controls. The results of the evaluation are in the form of the suitability of the controls on the weaknesses/vulnerabilities that are eliminated or reduced, as well as the effectiveness of the controls in reducing the risks that may arise as a result of these vulnerabilities/weaknesses; (3) The results of the cost-benefit analysis of the recommended security controls. The results of this analysis explain the benefits and disadvantages, if this control is implemented or not implemented, so that it becomes a consideration for information security planning; (4) The results of the cost-effectiveness analysis of the recommended safety controls. The results of this analysis explain the comparison of effectiveness between controls on the achievement of information security objectives, namely confidentiality, integrity and availability, thus providing a priority implementation proposal of all the recommended controls; (5) Security control plan, which contains the required resources that must be prepared to implement the security controls, as well as the team formed toimplement them.

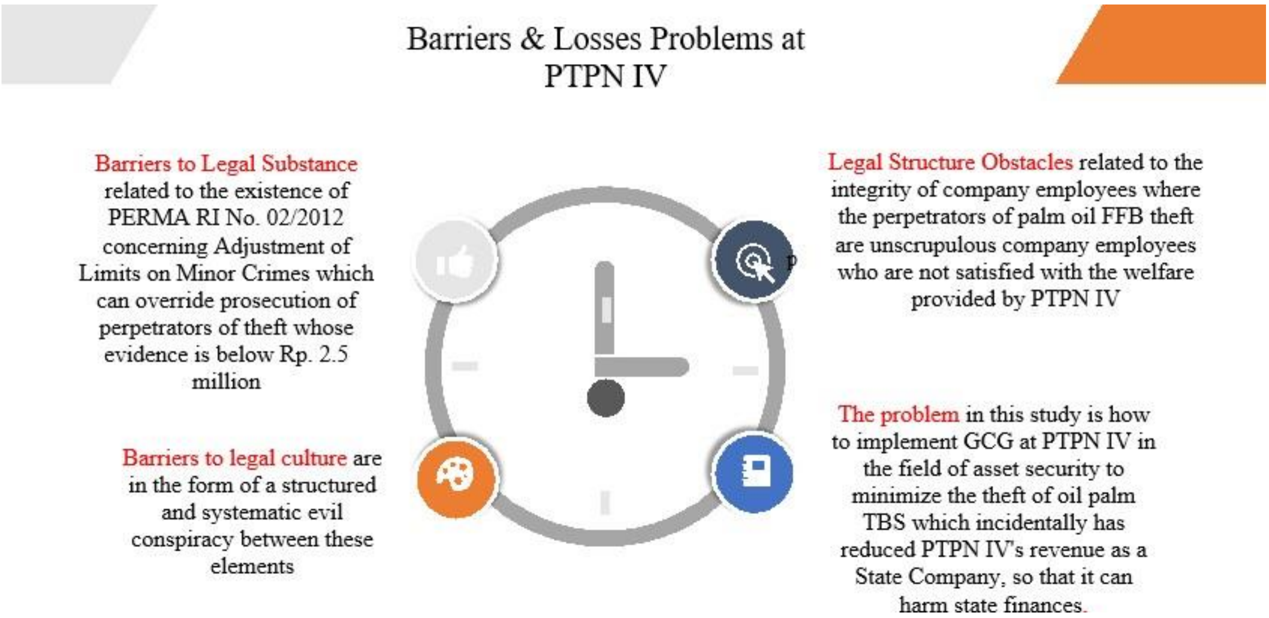
A comprehensive security plan has been prepared, based on the stages of risk assessment (risk assessment) and risk mitigation, so that it completely provides considerations and the basis for determining security objectives, targets, strategies and controls to ensure information security in the company.

Security controls are selected and used to achieve information security goals. There are three types of control used, namely management control (management control), operational control (operational control), and technical control(technical control).

The company's internal policies and controls in this security plan must be managed properly. Conner & Coviello, (2004) explains that information security governance is one part of the concept of good organizational governance, which consists of a set of policies and internal corporate controls that are coordinated and managed.

As for the facts found in the field, the mode of plantation crime is massive and organized. Regarding palm oil theft, many people assume that it is often carried out by palm oil ninja (simple crimes), but in reality theft by "palm ninja" is only about 10% up to 10%. 15% only. In reality, there is an oil palm mafia operating in PTPN IV plantations which accommodates up to 85% to 85% of the palm oil thieves. 90% (organized/serious crime). The oil palm mafias consist of: reservoirs, Youth Organizations (OKP), Non-Governmental Organizations (NGOs); RAMP; POM without gardens; intellectual actor; financier; drug dealer; unscrupulous employees; and backing. Weak security and law enforcement systems and lack of coordination with Law Enforcement Officials are the reasons for the theft and embezzlement of FFB (Report No. TBL/937/XII/2017).

The crime of theft and embezzlement of oil palm FFB in the PTPN IV area is massive and can be categorized as very critical (state of civil emergency). The theft and embezzlement of oil palm FFB can be likened to stage IV cancer that has spread to every important organ. The estimated value of losses suffered by PTPN IV is + IDR. 500 billion/year



Barriers & Losses Problems at PTPN IV

Barriers to Legal Substance related to the existence of PERMA RI No. 02/2012 concerning Adjustment of Limits on Minor Crimes which can override prosecution of perpetrators of theft whose evidence is below Rp. 2.5 million

Legal Structure Obstacles related to the integrity of company employees where the perpetrators of palm oil FFB theft are unscrupulous company employees who are not satisfied with the welfare provided by PTPN IV

Barriers to legal culture are in the form of a structured and systematic evil conspiracy between these elements

The problem in this study is how to implement GCG at PTPN IV in the field of asset security to minimize the theft of oil palm TBS which incidentally has reduced PTPN IV's revenue as a State Company, so that it can harm state finances.

Resistance

The obstacles that occur in the field include; (1) There is not a close relationship with law enforcement officers (Polri/Prosecutors and Courts), so that the perpetrators of the crime of FFB theft who often only get a TIPIRING verdict (minor crime) so that they never get a heavy verdict in court; (2) The occurrence of Coordination of Security in the field related to security & production SOPs; (3) There is no supervision over the implementation of SOPs for rewards and punishments that apply in each afdeling/plantation unit for arresting perpetrators of criminal acts of theft.

Public road access within PTPN IV garden

The status of the entrance to the plantation/company area is still mostly one with access to a village road or village road, making it easier for theft to occur in the plantation area belonging to PTPN IV.

Residential housing that is too close to the garden

Parameters or plantation boundaries that are not clear and tend to have no clear boundaries between private/community plantation areas and PTPN IV.

Threat

It is suspected that the FFB theft was carried out by community members around the plantation in collaboration with unscrupulous staff and employees of the company as well as company partners, as well as unscrupulous security personnel, both organic and BKO security personnel;

Based on Assessment I and Assessment II, FFB theft in the PTPN IV area is massive and in the very critical category (chronic disease stage 4) with a loss value of + 5 Tons/Day based on the classification + IDR. 216,000,000,000, - can be seen below the following table:

No	Loss Classification (±)	Total TBS/ Kg	Price TBS/Kg (IDR)	Day (month)	Total of garden	years (month)	Vehicle Type/ Others *)	Total (R2/R4)/ others **)	Total (IDR)
1	Minimum	23.740	1.200,-	30	20	12	Big/Mini Factory	-	205.113.600.000,-
2	Minimum	1.000	1.200,-	30	20	12	R4	2	8.640.000.000,-
3	Minimum	200	1.200,-	30	20	12	motorcycle rickshaw	2	1.728.000.000,-
4	Minimum	50	1.200,-	30	20	12	Motorcycle	5	432.000.000,-
5	Minimum	10	1.200,-	30	20	12	Resident	10	86.400.000,-
Total									216.000.000.000,-

Losses have been detected due to the occurrence of criminal acts of theft and embezzlement + IDR 216,000,000,000, -, with a minimum estimated loss of + 25 Tons/20 Gardens/Day, so that the security and security process is further tightened, this is done to minimize even greater losses due to the occurrence of criminal acts of theft in the PTPN IV area, can be seen below the following table:

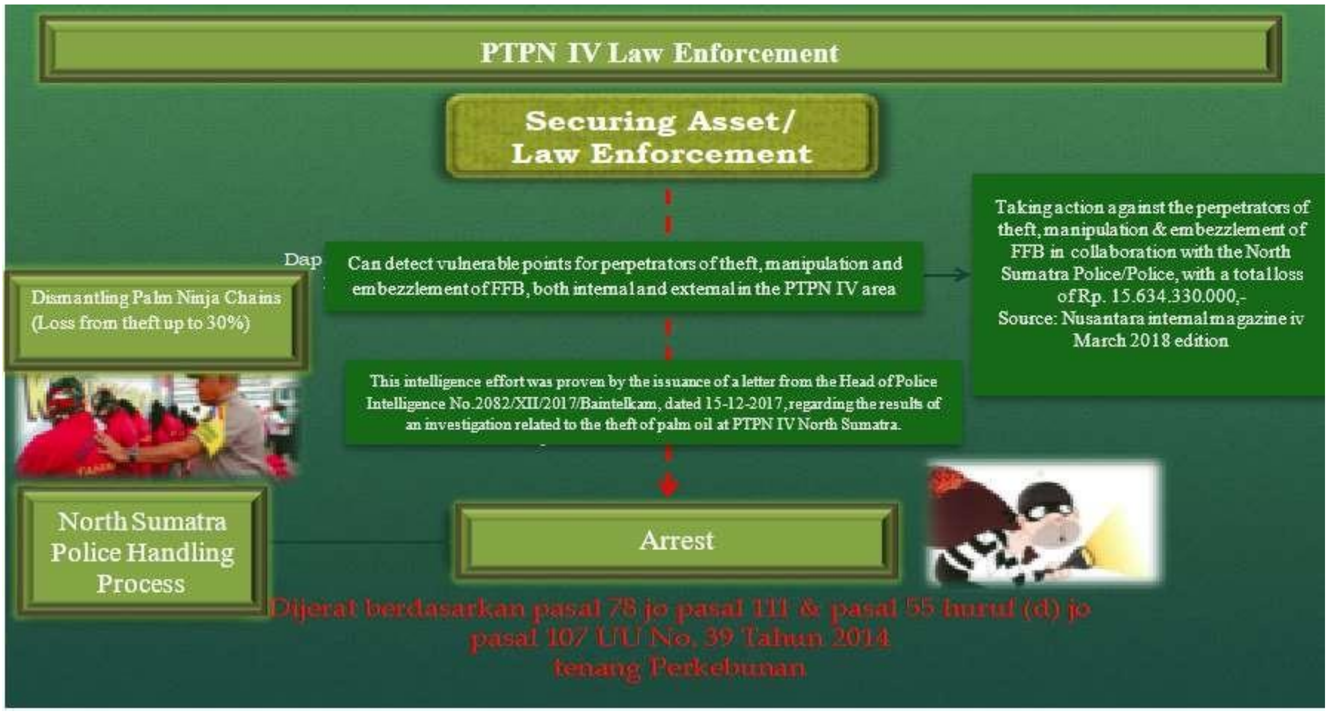
No	Loss Classification (+)	Total of TBS/day Kg	Price TBS/KG (IDR)	Total of garden	Day (month)	Years (month)	Total (IDR)
1	More or less	25.000,-	1.200,-	20	30	12	216.000.000.000,-
Total							216.000.000.000,-

Source: Letter from the Head of the National Police Security Intelligence Agency No: B/2082/XII/2017/Baintelkam, dated 15/12 2017, regarding: Results of Investigations related to Palm Oil Theft at PTPN IV Medan (Basic Assumptions Price of IDR. 1200/Kg is based on Police Headquarters Letter No: B/2082/XII/2017/Baintelkam, dated 15/12 2017, Number 2, letter (a) sub (6)).

Existence of Evidence of Report No: TBL/937/XII/2017/Bareskrim, dated 8/12/2017; concerning Reporting of Alleged Crimes of Harvesting or Collecting Plantation Products illegally as referred to in Article 107 letter (d) of Law No: 39/2014 concerning Plantations in conjunction with Article 55, so that they can invalidate their assumption that the perpetrators of criminal acts of theft and embezzlement consider that the law cannot be enforced for those perpetrators who commit criminal acts of theft and embezzlement at PTPN IV.

Letter from the Head of the National Police Security Intelligence Agency No: B/2082/XII/2017/Baintelkam, dated 15/12 2017, regarding: Results of Investigations related to Palm Oil Theft at PTPN IV, so that it can be used as a basic reference in catching perpetrators of criminal acts of theft and embezzlement committed by perpetrators that harm PTPN IV + IDR 176,000,000,000,-. Established coordination between Polri Headquarters and Polda/Pangdam/Kapolres/Dandim/Polsek/Koramil in handling and/or arresting criminal cases of theft and embezzlement in the PTPN IV area.

Closed and open security of the working area of PTPN IV in the context of intelligence activities aimed at supporting the implementation of the main tasks of the National Police carried out by applying procedures, methods, techniques and tactics in the form of preventive measures and direct, open or closed action against all forms of threats to ensure security and order around the PTPN IV area, in order to create a safe and orderly atmosphere and sterilize all forms of threats, disturbances, obstacles and challenges from the perpetrators of theft and embezzlement that occurred in the PTPN IV area, as for law enforcement actions carried out by the Police and Other law enforcement agencies against perpetrators of theft in the work area of PTPN IV can be seen in the picture below:



PTPN IV Law Enforcement

Securing Asset/ Law Enforcement

Dap

Can detect vulnerable points for perpetrators of theft, manipulation and embezzlement of FFB, both internal and external in the PTPN IV area

Taking action against the perpetrators of theft, manipulation & embezzlement of FFB in collaboration with the North Sumatra Police/Police, with a total loss of Rp. 15.634.330.000,-
Source: Nusantara internal magazine iv March 2018 edition

Dismantling Palm Ninja Chains (Loss from theft up to 30%)

This intelligence effort was proven by the issuance of a letter from the Head of Police Intelligence No.2082/XII/2017/Baintelkam, dated 15-12-2017, regarding the results of an investigation related to the theft of palm oil at PTPN IV North Sumatra.

North Sumatra Police Handling Process

Arrest

Dijerat berdasarkan pasal 78 jo pasal 111 & pasal 55 huruf (d) jo pasal 107 UU No, 39 Tahun 2014 tenang Perkebunan

The solutions to overcome the theft of PTPN IV assets are as follows;

Preventive Effort

Preventive efforts that can be done are as follows; (1) Increase garden security patrols (routine patrols once a day to three times a day) in areas prone to theft; (2) Installing additional security devices in areas prone to theft; (3) Empowering Pamswakarsa good social relations with the community in the community around the plantation; (4) Making elephant trenches and building forts in areas bordering villages where people live and places prone to theft. The aim is to make it difficult to move fruit out of the plantation area; (5) Blocking roads and installing portals with the aim of making it difficult for the perpetrators to lift or carry away their stolen goods; and (6) fostering a harmonious, balanced and harmonious household life leading to a harmonious family life (without stealing FFB).

Repressive Effort

Repressive efforts were carried out after the occurrence of a criminal incident in accordance with Law No. 39/2014 concerning Plantations, namely by imposing severe penalties for perpetrators.

CONCLUSION

Oil palm plantations play an important role in the national economy and have great potential in national economic development in order to realize the prosperity and welfare of the people in a just manner. Security Assessment is a measurement for a security model on a system in an organization or company (Miles, Rogers, Fuller, Hoagberg, & Dykstra, 2004). The security model is the way in which information system security is implemented in an organization. This measurement aims to provide information about the information system security gaps that exist in the organization or company which then the measurement results will be used to improve security. Immediately form an Independent professional team who are concerned about the progress of PTPN IV, macro on the more widespread and massive theft incidents in the PTPN IV area and conduct a review (review) of SOP Security and plotting the right members / in accordance with the correct security standards (experts in their fields), for cooperation contracts with vendors or third parties in terms of transportation of FFB integrated with the IT system, thus closing the possibility of cooperation that is detrimental to the company with parties both internal and external to the company within PTPN IV. Immediately carry out open security and closed security to prevent criminal acts in the PTPN IV area so that losses caused by rampant theft/ embezzlement and crime of TBS positions can be minimized by doing physical and non-physical refreshments to members of the TNI/Polri /Centeng/security as partners so that they have a positive relationship to coordinate security in the plantation area belonging to PTPN IV.

Forming an independent professional team to conduct a review of the allocation of CSR/TJSL/PKBL funds that are right on target and touch the hearts of the community around the plantation in order to develop a sense of belonging to the community towards the existence of the garden or PKS, so that will have a preventive impact on criminal acts so as to close access to illegal acts in the plantation environment belonging to PTPN IV.

Take firm action (without selective cutting) actions against the law for theft (theft/ embezzlement and office crimes by processing the money laundering crime (TPPU) of the FFB harvest belonging to the PTPN IV company until the court verdict level and also monitoring with other relevant agencies (TNI/Polri/Prosecutor) directly as a deterrent effect for perpetrators of criminal acts within the PTPN IV company environment.

Conducting good social relations with the community such as holding counseling about the danger/high threat of theft based on Law No: 39/2014 on theft. Letter from the Head of the National Police Security Intelligence Agency No: B/2082/XII/2017/Baintelkam, dated 15/12 2017, regarding: Results of Investigations related to Palm Oil Theft at PTPN IV, so that it can be used as a basic reference in catching perpetrators of criminal acts of theft and embezzlement committed by perpetrators that harm PTPN IV +IDR176,000,000,000,-

In addition, the results of the security assessment can actualize losses in the plantation area, it is necessary to carry out the following steps; (1) A comprehensive security plan has been prepared, based on the stages of risk assessment (risk assessment) and risk mitigation, so as to provide complete considerations and the basis for determining security objectives, targets, strategies and controls to ensure information security in the company; (2) Perform selected and used security controls to achieve information security objectives. There are three types of control used, namely management control, operational control, and technical control; (3) Controlling the company's internal policies and controls contained in this security plan, must be managed properly in accordance with good organization governance, which consists of a set of policies and company internal controls that are coordinated and managed based on policies. Company Directors.

REFERENCES

[1] Conner, F. W., & Coviello, A. W. (2004). Information security governance: a call to action. *The Corporate Governance Task Force*, 3-49.

[2] Davis, J. I., Libicki, M. C., Johnson, S. E., Kumar, J., Watson, M., & Karode, A. (2016). *A framework for programming and budgeting for cybersecurity*. RAND Corporation Santa Monica United States.

[3] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. serwiss.bib.hs-hannover.de

[4] Gultom, R. A., Kustanaand, T., & Bura, R. O. (2018). Enhancing Computer Network Security Environment by Implementing The Six-Ware Network Security Framework (SWNSF). *Computer Science & Information Technology*, 153-166.

[5] Mell, P., & Grance, T. (2002). *Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme*. National Inst Of Standards And Technology Gaithersburg Md Computer Security Div.

[6] National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cyber Security. U.S Departement ofCommerce.

[7] Podungge, D., Mashudi, I., & Napu, K. (2020). Analysis of Performance Assessment System Model of Civil Servants in Gorontalo Province Training and Education Agency. *Journal La Sociale*, *1*(4), 27-32. https://doi.org/10.37899/journal-la- sociale.v1i4.143

[8] Shrestha, N. (2012). *Security Assessment A Network and System Administrator's Approach* (Universitas Oslensis)

[9] Sikumbang, J. (2010). *Mengenal sosiologi dan sosiologi hukum*.
Medan: Pustaka Bangsa Press

[10] Triningsih, A. (2016). Hak Konstitusional Masyarakat Hukum Adat Dalam Judicial Review Undang-Undang Perkebunan. *Kajian*, *18*(3), 203-215.

[11] Yunanri, Y., Riadi, I., & Yudhana, A. (2017, February). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). *Annual Research Seminar (ARS)* *2*(1). 300-304.