Americans Journal of Open Research , 2(12), December, 2023, 839-855
E-ISSN: 2834-7668

STRATEGY FOR STRENGTHENING NATIONAL POLICE PUBLIC SERVICES BASED ON INFORMATION TECHNOLOGY THROUGH A DATABASE MANAGEMENT SYSTEM

R. Dwi Chandra Narisa[1]*, Riska Sri Handayani[2], Lim Yola[3]

[1,2,3] *University of Indonesia, West Java, Indonesia*
e-mail: r.dwi11@ui.ac.id [1], riska.sri@office.ui.ac.id [2] ,lim.yola@office.ui.ac.id[3]*

* Corresponding Author

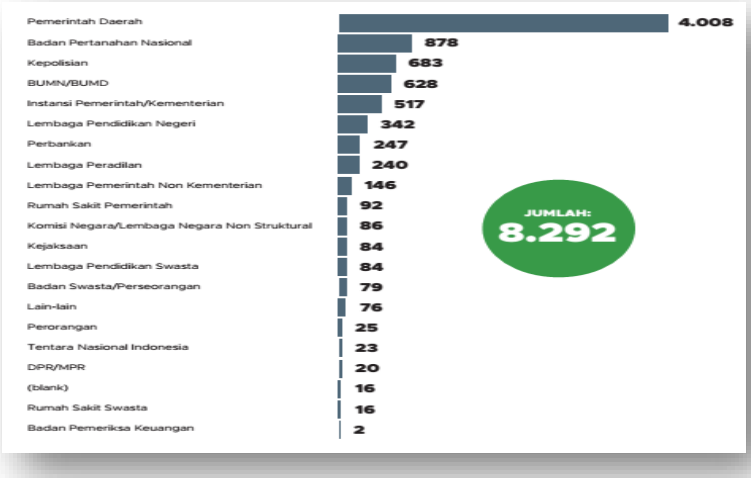
Abstract: *The research aims to examine the Indonesian police strategy to improve technology-based public services in relation to complaints of unprofessionalism by members of the National Police. This research is qualitative research with primary data sources directly from the Indonesian police and secondary data from various sources relevant to this research. The results of this research explain that the Polri's strategy in improving public services to the community is related to the unprofessionalism of Polri members, strengthened by using the Polri database management system. This system saves data that has been stored in old filling & recoding applications. Developing new applications that are integrated with each bureau and can be accessed by all regional police to regional police. The focus of the research that will be carried out by researchers, which is different from previous researchers, lies in an in-depth study of the number of alleged abuses of authority committed by Indonesian police officers and the unprofessionalism of the positions they are currently holding through the Divpropam Polri Database Management System.*

Keywords: *Strategy, Indonesian police, Database management System,*

INTRODUCTION

As a government institution, the National Police in this case has an important role in developing electronic public services that are comprehensive, integrated and accessible to the wider community. Presidential Regulation Number 95 of 2018 sets the government's goal as implementing a comprehensive and integrated electronic-based government system to facilitate high-performance public services and bureaucracy. This goal is in line with the role of law enforcement which is one of the government's responsibilities in the areas of maintaining security, law enforcement and bureaucratic efficiency of services related to the community.

The contradiction between high levels of public complaints and public services that are considered less than optimal is a problem often faced by many institutions. This phenomenon illustrates the gap between people's expectations of public services and the reality of their implementation. Based on data from ombudsman reports related to the agencies that are most frequently reported by the public regarding public service issues, they include the following:



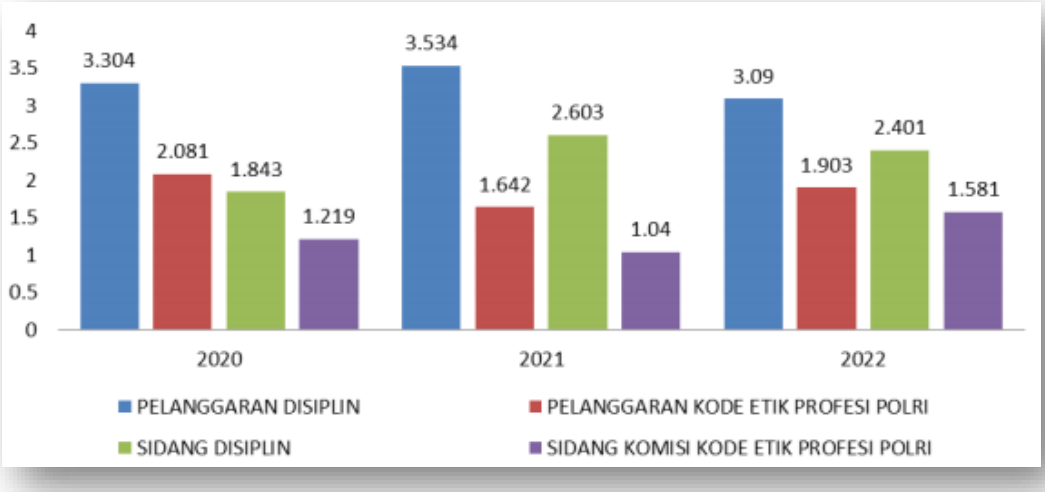
Source: 2022 Ombudsman Report

DOI:
https://opsearch.us/index.php/us/index

Figure 1. The most frequently reported agency community in public service matters

Based on data from the 2022 Ombudsman report of the Republic of Indonesia, the police institution was ranked third with 683 reports. In detail, the report concerns alleged maladministration of public services and the "sluggishness" of law enforcement carried out by the Republic of Indonesia Police. "During 2022 the number of reports related to the police consisted of 28 reports to the National Police Headquarters, 186 reports related to the Regional Police, 374 reports related to Resort Police and 95 reports related to Sector Police." (2022 Ombudsman Report). The data from the Ombudsman of the Republic of Indonesia regarding irregularities committed by the National Police institution tends to be in the administrative sector in the service sector, one of which is the service of public reports to the National Police Propam regarding alleged violations of discipline and code of ethics committed by National Police personnel.

Referring to the objectives of SPBE, Divpropam is making efforts to improve public services in receiving and handling public complaints with an integrated system, building a Database Management System Program or DMS Propam. DMS Propam is an Information Technology-based program to optimize the system for monitoring and controlling the performance of National Police members, so that the entire service process and handling of public complaints can be monitored by the National Police leadership. Based on public complaints and data collected by the National Police Divpropam for 2020-2022 regarding violations committed by National Police personnel, including the following:



Source: Divpropam 2023 report

Figure 2. Graph of Police Member Violations

From the table and graph above, it can be seen that the level of disciplinary violations by members in the last three years is still very high, and will only decrease slightly in 2022. Likewise, violations of the National Police's professional code of ethics are still almost consistent, although there has been a decline but it is not yet significant. Meanwhile, the number of disciplinary hearings has increased significantly from 2020 (1,843) to 2,603 in 2021, and decreased slightly in 2022 to 2,401. Likewise, code of ethics commission hearings have relatively increased from 1,219 in 2020 to 1,581 in 2022. On the negative side, this graph illustrates that the level of member violations, both disciplinary and code of ethics violations, is relatively consistent, with no significant decline in the last three years. Meanwhile, the positive side is that the violation process continues to increase, both

through disciplinary hearings and professional ethics commission hearings for the police, and this illustrates the level of seriousness of the police in enforcing discipline among its members. The highest disciplinary violations occurred in 2021, namely 3,534 violations, while the highest violations of the National Police's professional code of ethics were in 2020 with 2,081 violations.

With the DMS Propam Indonesian police, it can make it easier to resolve various public complaints systematically. Even though in fact the implementation of DMS Propam can work, there are still many obstacles faced, both in terms of systems, human resources and policy implementation that cannot be implemented optimally. Another weakness faced regarding the implementation of DMS Propam is also related to its status which originates from a cooperation agreement in the form of providing a grant from the US government to the National Police and from the aspect of data security which is still very vulnerable, this is because the management and development of the system still involves third parties, so In the end, Propam's DMS has been temporarily suspended in order to make systemic and managerial improvements.

The focus of the research that will be carried out by researchers, which is different from previous researchers, lies in an in-depth study of the number of alleged abuses of authority committed by members of the National Police and the number of unprofessionalism in the positions they are currently holding through the National Police Divpropam Management System Database. Then, from the results of this study, researchers will try to formulate a model for strengthening accountable and transparent performance as an effort to increase *public trust in society.* This is the background for the author to carry out in-depth research regarding the Strategy Study for Strengthening National Police Public Services Based on Information Technology. So based on the explanation above, the questions to be answered are as follows: How does the National Police's strategy to improve technology-based public services relate to complaints of unprofessionalism by members of the Indonesian National Police?

METHODS

This research uses a descriptive method with a qualitative approach, namely "to understand certain social situations, events, roles, groups or interactions (Creswell, 2002). In general, this paradigm is an investigative process in which researchers gradually try to understand social phenomena by differentiating, comparing, imitating, cataloging and grouping study objects. In the context of this research, it is hoped that the study of information technology-based strengthening strategies for the National Police's public services using the Case Study of the Divpropam Indonesian police Database Management System (DMS) will provide a comprehensive and in-depth picture regarding the process of implementing the Divpropam Indonesian police Database Management System (DMS). This aims to enable researchers to analyze it in depth and provide a clear analysis of its application, so that they can obtain research results that can become recommendations for future policy.

Primary data is a source of data obtained directly from original sources (not through intermediary media). Primary data can be in the form of opinions of subjects (people) individually or in groups based on interviews, results of observations of objects (physical), events or activities, and test results. In this research, primary data sources were obtained from interviews with informants and sources who know the ins and outs of implementing the Database Management System (DMS), which consists of policy makers, field implementers, reporters and observers/experts. Then other primary data was obtained during direct observation at the National Police Divpropam. "Secondary data is a source of research data obtained by researchers indirectly through intermediary media (obtained and recorded by other parties). Secondary data generally takes the form of evidence, notes or historical reports that have been compiled in published and unpublished archives (documentary

data). Secondary data in this research can be in the form of a basic report on the duties of Divpropam Indonesian police, the results of policy formulation meetings or the annual report of Divpropam Indonesian police.

THEORETICAL FRAMEWORK

Information Technology

In the current information era, organizational leaders are looking for ways to use information technology (IT) to support their strategies in improving service and organizational performance. Information technology facilitates an organization's ability to predict and respond quickly to market or environmental changes (Porter, 1985: 88). The dynamics of environmental change create many opportunities and threats for organizations. Therefore, most organizations try to know and follow environmental developments so that the organization can reduce uncertainty and facilitate effective decisions (Dallaire, 1992: 43).

Information Technology is a very important tool available to leaders to help them face the challenges of change. Apart from that, information technology is becoming more important, because information technology can be the glue that unites organizations together and helps leaders to control and develop the organization (O'Brien, 2001: 65). Information technology also acts as an information system, so that the two dimensions of information systems and information technology have a relationship that strengthens organizational services.

Information Technology is defined as "the various technologies that are used for the creation, acquisition, storage, dissemination, retrieval, manipulation and transmission of information (Jimba, 1990: 12). Information technology is used to create, obtain, store, disseminate, search, manipulate and transmit information. It seems that this definition has similarities with the definition given by the British Department of Industry which states that information technology is the acquisition, process, storage, dissemination of sound, images, text and numerical information based on a combination of microelectronics which is a combination of computing and telecommunications. (Suleiman A. Al Khatttab, 2005:78). Information technology represents various types of "hardware and software" used in information systems including computers and network equipment (Post and Andersen, 2000: 102). Management Information System Solving Business Problems with Information Technology. Second Edition. McGraw Hill, USA.

Concept of Police Professionalism

Police professionalism is the basic foundation for professional institutions including the police. The professionalism of the police can be seen, measured and felt significantly as a result by the community, namely the guarantee of safety and security of citizens in their activities. With this guarantee, the community will feel safe and comfortable in carrying out activities that can improve their lives. Good performance products in the form of conceptual, managerial, operational and improving people's quality of life will show professionalism. This must be accounted for at levels that are adjusted to the context or scope of each task. Both administratively, legally and even morally at the same time.

Police professionalism is the basic foundation for professional institutions including the police. In order for the police to thrive and develop, policing is to create and maintain social order in society, prevent security disturbances, build partnerships and make efforts to improve the quality of life of the community. According to Kastorius Sinaga (2008:96): "Police professionalism does not only mean increasing the technical capabilities of police officers at the micro/field level. However, there is a fundamental change in the paradigm of the police institution, capable of becoming an independent civil institution and implementing the concept of democratic policing.

In the context of the Police as a democratic civil police, the police are able to uphold the supremacy of the law, provide guarantees and protection of human rights, are transparent and

accountable, and are oriented towards improving the quality of life of the community. Of course, it is not a tool of the authorities or an autonomous branch of power without public accountability (Maridjan, 1999, Sinaga 2008).

Police professionalism further requires developing the integrity of all police officers and their functions by implementing or adopting modern management principles with performance that is measurable and open to be assessed by the public, as well as accountability (Suparlan, 2005, Chryshnanda , 2009). If democratic principles are not developed within the police organizational culture, it could lead to error, especially in the use of authority, especially in discretionary actions. Bayley (1988:77) states that excessive discretion is a big potential for corruption. In a constitutional state based on law (rechstaat), the professionalism of the police as the spearhead in law enforcement is highly demanded. Important elements in building police professionalism include:

a. Integrity, Spirit and Skill

"Don't place the wrong people, or place people who don't have character because it will damage the institution."

According to Chrisnanda (2002: 88), developing and placing human resources with character requires art and skills (art and skills). The main asset of an institution is not only human resources but human resources with character. Selecting, placing and using human resources with character requires the right sensitivity and feeling. Of course, based on competence and performance. Apart from that, you also need an interview before promoting. Promotion is not a secret for human resources officials or certain officials, except in patrimonial bureaucracies. It can be said that officials in the human resources sector have no time to interview or look for human resources with character. In a patrimonial bureaucracy it is actually sacred and considered an angel of death. Because the approach is a personal approach.

Determining human resources with character is not just about issuing an order but also as a form of cadre formation so that in the future we will have human resources with character (professional, superior and ethical). In determining a person's character, there are 3 main provisions whose sequence (Chryshnanda, 2009:23) are:

1.Integrity.

2. Spirit and

3. Skills.

In irrational bureaucracy and corruption, people of character will consciously or unconsciously be killed, removed, because they are considered a threat, as a nuisance to their privilege. Because the core value is money, Collusion, Corruption and Nepotism (KKN) is rampant and thrives. People of this character will continue to be pushed aside at all levels. So over time they were finished because there was no land for them to grow and develop.

Institutions that have people with character will be able to survive and compete and even excel. Even countries that have a lot of human resources with character will become superior and dominate the world. They are not easily influenced, not easily overthrown, because their power is rooted everywhere. Quick to rise and be able to become a role model everywhere, inspiring, motivating, of course because of being professional, superior and ethical.

b. Leadership

Leadership from all leaders at various levels who are able to apply visionary, transformative, innovative, creative leadership full of motivation to build professional, intelligent, modern police institutions as civil police in a democratic society. The values and systems they build can be said to be

temporary, reactive, partial, and may even leave the birth of time. Today's mistakes are killing future generations.

c. Cultural Values.

The police cultural values that are used as a frame work or faith for police members are humanism, awareness, responsibility as part of the spirit that protects life. The core values of National Police professionalism are the core values which are the main categories of the value *system* . A value system is a set of consistent ethical (moral) values and more specifically personal and cultural values. And the measurement standards (*clarification needed*) in achieving ideal goals both ethically and ideologically (Chryshnanda, 2009:98).

Cultural values are values that are agreed upon and embedded in a society, organizational sphere, community environment, which are rooted in habits, beliefs , symbols, with certain characteristics that can be distinguished from one another as a reference for behavior and response to what will happen or is happening.

Cultural values will appear in symbols, slogans, mottos, vision and mission, or something that appears as the main reference for the motto of an environment or organization. There are three things related to these cultural values, namely: Symbols, slogans or other things that are visible to the naked eye (clear). Attitudes, actions, movements that arise as a result of the slogan, motto. Embedded beliefs (believe systems) that are rooted and become a frame of reference in acting and behaving (not visible).

An institution has goals and objectives to be achieved, which are reflected in its vision and mission. Professional institutions will have high work standards which serve as work guidelines for their officers or officials. For institutions that do not have standards or have low standards, they are usually unprofessional and can be said to be haphazard and there are many opportunities for deviation. The lower the standards of an institution, the lower the quality of performance, and vice versa, the higher the standards, the higher the quality of performance. The higher the standards, the more disciplined and compliance with product performance standards can be said to provide quality assurance of quality. The higher the quality of performance, the better it will be able to beat other competitors. This does not only apply to institutions but also to society, even nations and countries.

RESULTS AND DISCUSSION

1. Database Management System

Data consists of a compilation of factual information from the physical world, representing entities such as customers, employees, students, products, events, and concepts. It is usually represented in a variety of formats, including text, images, numbers, letters, symbols, or a combination of both. A database is a combined compilation of interconnected data stored on standard media. It should be free of duplicate entries to facilitate reuse and be optimally utilized by one or more application programs. In addition, data storage should not create dependencies on programs that want to access it. Furthermore, if additional data is needed, retrieval and modification can be carried out easily and in a controlled manner (Whinston, 2012: 43).

A Database Management System (DBMS) is a coordinated collection of tables or files stored in a database. It also consists of a collection of programs that allow multiple users or other programs to interact and modify this table (Whinston, 2012: 47).

A Database Management System is a computerized system whose main objective is to maintain and provide access to information, as stated by Date (2004:11). Composed of the following elements, the Database System functions as an integrated data file preparation system:

1. *Database* (Database)

2. *Software* (Software)
3. *Hardware* (Hardware)
4. *Brainware* (Human)

According to Miroslaw (2004: 497) the advantages of using a database management system:

1. Data can be used together (*Multiple Users*)
2. Data can be standardized
3. Reduce duplicate data (*redundancy)*
4. There is independence (freedom) of data or independent data.
5. Guaranteed data security (*Security)*
6. Data integrity is maintained (*Integrity*)
7. Speed and convenience
8. Data accuracy and data availability.

A Database Management System (Chassiakos, 2008:867) is reliable when it can guarantee, among other things, consistency and the absence of data redundancy. This can only be done when the information is highly structured. To give an example, a management information system based on the exchange of information via email can guarantee that information is transferred quickly and economically but there is little or no information about the information contained in the email. As a result, it is possible that information discrepancies (conflicting information in different emails referring to the same subject) or data redundancy (the same information repeated in different emails) may arise.

The proposed system is a web-based information and communication management system that aims to include general information circulating in the construction process. System development is based on emerging new technology from databases integrated in web applications. Database technology can reasonably organize large volumes of information, such as that generated during the construction process, while internet technology can instantly and with almost no cost and disseminate information throughout the world with no temporal or spatial boundaries.

The user-interface facility provides an input display that allows users to interact with the system via the world wide web using an internet browser; input/edit is a data input, update, and delete component developed to facilitate data entry and editing; The evaluation component assesses cost and schedule variances using the *earned-value method* (As Shawi, 2003:355).

The implementation of the database (Miroslaw. 2004: 497) would be better if it was packaged in web form as part of the *management tool* itself. This will be useful at various stages of the project life cycle, including:

a. Tender Stage

1. Increase the speed of distribution of tender documentation and communication
2. Online registration of tender participants and downloading work packages electronically
3. Provide a simple system for evaluating tender participants' responses through existing templates
4. Avoid unwanted access through security mechanisms
5. Communicate changes in tender documents during the tender process quickly and easily.

b. Design and Construction Phase

1. Reduce the risk of errors and rework by ensuring all members of the project team work with the latest documents or drawings
2. Save time in queries (requests for information) and approval processes by following existing online information
3. Eliminate the risk of losing critical data by maintaining all past and present data in one central location
4. Improve team communication by making it possible to obtain and respond to queries
5. Maintain all communication records for monitoring purposes (facility audit)
6. Providing a collaborative work environment for different members can be done via the web.

c. Material Purchase Stage and Project Requirements

1. Save time in material procurement with automatic distribution and communication documents (E-Procurement)
2. Reduce administrative costs from document handling and distribution to several groups
3. Reduce errors in effective communication
4. Make it easier to ensure comparison and evaluation of offers.

It is important for the database to have certain features and think about how these features will interact with the work tasks of the project team members. This feature will be useful as (Miroslaw. 2004: 451):

a. Document Management
b. Project Work Flow
c. Project Directory
d. Log control center
e. Fast search
f. Conferences and *white-boarding*
g. Sequential *online* discussions
h. Scheduling
i. Project camera
j. Data conversion
k. Printing service
l. *Website* customization
m. *Offline* access
n. Information Services
o. Project Information Archives
p. *E-Bidding & Procurement*

2. Cyber Security

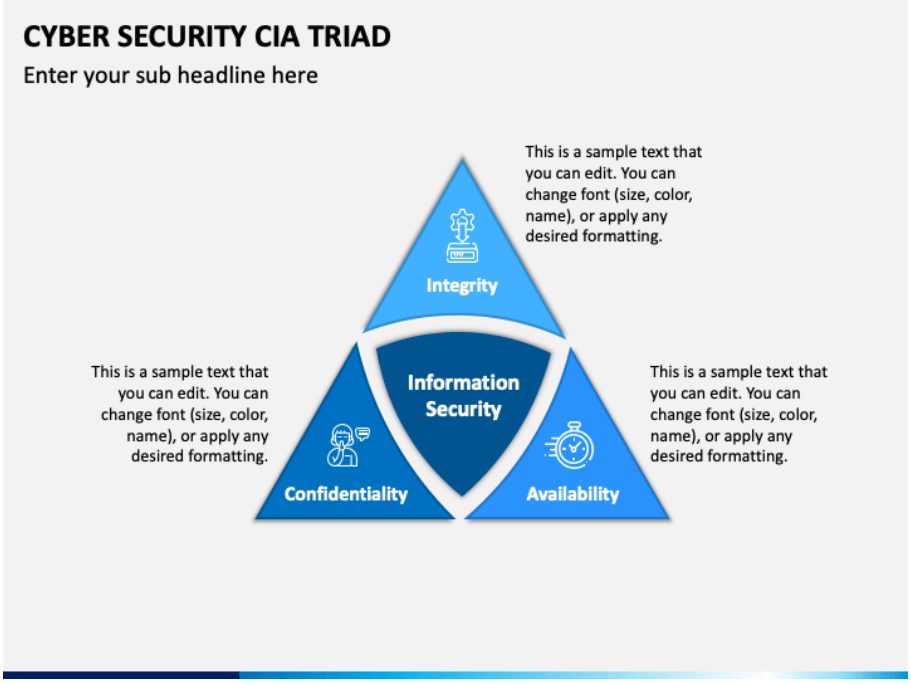
Cyber security can be interpreted as security in the realm of information technology which focuses on protecting computers, networks, programs and data from cyber attacks. Meanwhile, according to ITU-T Assets here include software and hardware used in cyberspace. There are 3 (three) important components in cyber security, namely confidentiality, integrity and availability. Cybersecurity is also defined as computer security and securitization (Hansen & Nissenhaum, 2009).

Implementation of cybersecurity measures ensures the protection of the digital world. This domain includes many public and private sector participants, each of which implements different strategies. Maintaining information security is greatly influenced by cyber security, because it is very important to protect data stored on storage media and ensure the integrity of the information transmitted (Damar, 2018). In addition, maintaining privacy is the most important thing in this domain because of the great influence of privacy protection on user trust.

Organizations that want to improve their cyber security can use the Sliding Scale as a metric to classify the actions, competencies, and allocation of resources that their personnel can use to protect themselves from cyber threats (Lee, 2015). Additionally, this report can serve as a structure for understanding potential steps that can be implemented to improve cybersecurity. In addition to ensuring the accuracy of root cause analysis of incidents, prioritizing and monitoring investments in resources and skills, and measuring security posture, Sliding Scale is a valuable tool for communicating technical security issues to non-technical individuals.

In the latest developments in cyber security discourse, the CIA triad concept has emerged which is used by the information technology industry to ensure data security from cyber attacks. The CIA Triad is a widely used information security model that can guide organizational policies aimed at maintaining data security. The model has nothing to do with the US Central Intelligence Agency (CIA); on the contrary, the initials of the abbreviation stand for three principles (Fruhlinger, 2020:2):

1. Confidentiality : *Only* authorized users and processes can access or change data
2. Integrity *:* Data must be maintained in a correct state and no one can modify it incorrectly, either accidentally or maliciously.
3. Availability : Authorized users must be able to access data whenever they need to do *so*



Source: CIS Center for Internet Security 2022
Figure 2.CIA TRIAD pyramid

According to Randeree (2006: 132), the CIA triad became famous in the information technology industry because every organization needs data security. In the past, the focus of cybersecurity was protecting and securing computer hardware, and it was easier to implement physical security controls for *hardware infrastructure* . As more users use computers and information technology resources, organizations are realizing that security and privacy controls such as access controls are necessary to limit misuse of data and protect information systems, leading to a shift from a primary focus on protecting computers physically to protecting software, applications, and data (Dhawan, 2014).

The foundation of the CIA triad consists of aspects of confidentiality *,* integrity *and* availability of data and information sources *(* Samonas & Coss, 2014). Zwick and Dholakia (2004: 89) define confidentiality *as* the perceived ability to limit the flow of information by preventing access to people. Threats to confidentiality are intruders, social engineering, insecure networks, and poorly designed systems. Integrity is *the* guiding principle at all levels of confidentiality. Data integrity ensures that data is in the most trustworthy state. Data integrity minimizes or eliminates the risk of physical data, which is often lost due to human error, *bugs* and viruses, lack of system security, and data corruption during data storage or transfer between devices.

Information providers ensure that data is available and can be accessed properly by recipients or users. Dhawan (2014 : 53) adds that access control is critical to achieving CIA security objectives and can be implemented through identification, authentication, and other authorization steps. Policies and regulations regarding user privacy should focus on application security to ensure secure coding, privacy by design principles, installation of firewalls, intrusion, detection and prevention systems against viruses. So that an organization must comply with the basic requirements of the CIA triad invariably affects the quality of the security rules and procedures implemented, leaving the organization vulnerable to system breaches and insider threats.

To include concepts such as accountability *,* audibility and authenticity *(* Haubinger, 2015: 67). According to this improvement, information systems include monitoring and enforcing user actions in the network and streamlining information system user activities to comply with all provisions (Haubinger, 2015). Continuous monitoring activities prevent and manage potential data breaches that would otherwise result from intentional and unintentional actions. Information systems have traditionally been discussed in the context of the CIA model and serve as benchmarks for evaluating information systems and security systems (Jonnaganti, 2009: 89). The main goal of information systems is the protection of organizational assets from business operations that compromise data security (Caballero, 2014: 88).

According to Gladden (2017 : 70), this protective action is data and information systems that are protected from access, use, disclosure, interference, modification and destruction to ensure that CIA objectives are met. To elaborate further, Solms and Niekerk (2013) note that "information security" has been used interchangeably with the term "cybersecurity". So that the concept involves the entire information system and is primarily focused on protecting information resources which is a continuous process and also a product of interactions between people, policies, procedures, processes and technology (Rao & Nayak, 2014).

Chaeikar et al. (2012 :77) concludes that the CIA model conceptualizes a data information system that can be trusted and protects data from unauthorized use. Critics argue that the CIA's triad goals are somewhat limited and do not take into account emerging threats in the information technology industry (Cherdantseva et al., 2013; Whitman et al., 2011). As a result, efforts to improve the pitfalls associated with the CIA model resulted in the proliferation of alternative models such as the Information Assurance and Security Reference Model and the Integrated Security Management SOA Model (Cherdantseva et al., 2013; Jonnanganti, 2009).

Apart from the CIA Triad concept, what is included in the scope of *the Cyber Security Theory study* is *the Intrusion Detection System* (IDS) and *the intrusion prevention system* (IPS). *Intrusion Detection System* (IDS) is a security device installed on a computer network. Unlike *firewalls* , IDSs are usually placed within a network to monitor all internal traffic. IDS is an intrusion detection process that can be managed autonomously to find violations of security policies or security incident practices in computer networks (Kim, 2018: 77). In general, IDS is tasked with monitoring network traffic, notifying if an intrusion occurs, and documenting it in *a log* . This is different from the job of *a firewall* which also blocks unwanted data packets. However, currently there are many devices circulating that combine the functions of IDS and *firewall* .

To improve cyber security, organizations can use the Sliding Scale as a metric to categorize the competencies, actions, and distribution of resources that their personnel can use to counter cyber threats (Lee, 2015). Additionally, this report can serve as a framework for understanding possible prospective steps to improve cybersecurity. The Sliding Scale serves as a valuable instrument for communicating technical security concerns to non-technical individuals, in addition to prioritizing and monitoring investments in resources and skills, ensuring the accuracy of incident root cause analysis, and measuring security posture.

Based on the detection method, IDS can be divided into two different types, namely misused - *based IDS* or also known as signature-based IDS *and* anomaly- *based IDS* . Abuse or signature-based IDS searches for the presence or absence of attack activity by matching signatures or label characteristics or patterns of previously stored attack activity. This type of IDS is suitable for detecting previously known attacks, but has weaknesses in detecting new or previously unknown attacks. Meanwhile, anomaly-based IDS can detect attacks by identifying network behavior or characteristics during normal use and will provide notification if there are differences from that (Othman, 2018: 99). This type of IDS can detect new or previously unknown types of attacks. Abuse or signature-based IDSs typically produce higher detection accuracy performance on known attack types than anomaly-based IDSs. In general, the comparison between the two types of IDS is summarized in Table 2.1. as follows :

Table 2.1.

Comparison of IDS based on detection methods

	Abuse-based IDS	**Anomaly-based IDS**
Detection method	Identification based on known attack patterns	Identify unusual attack patterns
Detection rate	Tall	Low
False alarm rate	Low	Tall

Ability detect unknown attacks	Unable	Capable
Another weakness	Must always renew signatures	Performing *machine learning computations* in real-time requires lots of resources and time.

If you look at the comparison of the two types of IDS, each has advantages and disadvantages that can be adjusted to security needs. However, if you look at the many new types of attacks that emerge all the time with attack techniques that continue to develop, then the use of anomaly-based IDS can be considered. Then, to improve the IDS's ability to detect attacks, machine learning techniques *are* often used in anomaly-based IDS research because of the nature of their ability to learn attack patterns (Pilli, 2019: 45).

After that, intrusion prevention systems (IPS) were the next idea. IPS is able to identify suspicious activity through network traffic monitoring and network protocol analysis. The Intrusion Prevention System (IPS) generates reports, notifies administrators regarding the security of the observed object, and documents information specifically related to the observed object. Many intrusion prevention systems (IPS) are also capable of addressing threats to prevent system intrusions. They implement a variety of responses to threats or intrusions, such as intrusion prevention systems (IPS) capable of thwarting threats directed at the organization itself, modifications to system security measures (e.g., firewall reconfiguration), or changes in the nature of the intrusion or intrusion. threat content (Zhou, 2020: 87).

An intrusion prevention system (IPP) is a procedure that utilizes intrusion detection to thwart potential events that may occur. The primary objectives of an Intrusion Prevention System (IPS) are as follows: identify potential intrusions or threats, notify network administrators of logging information related to such intrusions or threats, devise strategies to impede their progress, and report the information to the administrator. IPS is also used by businesses and organizations for a variety of purposes, including detecting violations of computer network security policies, documenting emerging threats, and preventing individuals or entities from violating those policies. IPS is a critical component of any organization or business's computer network security infrastructure.

Intrusion detection system (IDS) software automates intrusion detection. Software that has complete capabilities to not only identify system intrusions but also prevent potential harm or intrusion is referred to as IPS. IDS and IPS technologies collaborate to provide a variety of functions, and when an IPS product operates as an IDS, the network administrator can usually disable the prevention function.

Zhou (2020) describes various categories of intrusion prevention system (IPS) technologies, where the main differences lie in the classification of threats that can be detected and the techniques used for threat identification. In addition to monitoring and analyzing events to identify unwanted activity, all types of IPS technology typically perform the following functions. The following functions:

1. Start by documenting events related to the observed phenomenon. Information can be sent to separate systems, including centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems, in addition to typically being stored locally.
2. Communicate the significance of the observed event to the security administrator. This form of communication, referred to as an alert, can be delivered via email, web page, IDPS user interface

message, SNMP, and other means. The notification message category contains only basic details about an event; administrators need this information to gain access to IDPS for further information.

3. generate reports. In the report, supervision of an event is concluded or provided with specifics regarding the event.

3. **Indonesian police strategy to improve technology-based public services**

The resources owned by the organization, whether in the form of human resources, budget or infrastructure, are important elements for the National Police which can determine optimal performance in dealing with criminal acts of terrorism through the use of the National Police's database management system. Human resources are an important asset in responding to complaints through the use of the National Police database management system.

The importance of human resource management in running an organization to achieve goals optimally is an inseparable necessity, so the basic things that need to be looked at are HR Planning, Recruitment and Selection and Education and Training. In the context of this research, these three aspects are connected to the National Police database management system.

Based on the results of field research from the aspect of HR planning for users of the National Police database management system; the category of preparing and planning regulations, guidelines and work procedures in the field of HR management can be implemented even though not yet synergistically so that it can be used as a reference in making organizational policies within the National Police. However, the categories of preparation, study, development and implementation of the HRM system used by the organization are not running optimally, plus there is a lack of an evaluation system for the National Police database management system.

By looking at information from sources that the National Police's database management system user recruitment system does not use competency as the main basis, the tendency is for the National Police to conditionally determine the position of users of the National Police's database management system, thus the operational function of human resource management does not run optimally so that Optimization efforts can be made by starting with improving the recruitment system and appointing users of the National Police database management system. Seeing that the contribution is quite large, the use of the National Police database management system is where this system helps in handling public complaints against deviant police officers.

Apart from the human resource management aspects above, other resource availability factors are also very important to encourage the optimization of human resources, at least several aspects include;

The ideal human resource aspect can be fulfilled if the composition of personnel in the National Police, especially those tasked with being operators of the National Police's communication network system in the form of the National Police's Database management system, eADS, SDWAN, TV Monitoring, PID, database, VOIP and Facsimile. The addition of personnel is intended to ensure that there are no double *job desks* for operators of the communication network system, so that with the increase in operator personnel, especially for the National Police database management system, it is hoped that; *Firstly,* operators do not work in multiple positions. *Second,* the National Police database management system can operate 24 hours because there are operators who work in *shifts.*

The relationship with the National Police's database management system workflow can be described as follows:

Picture 3
National Police DMS Workflow

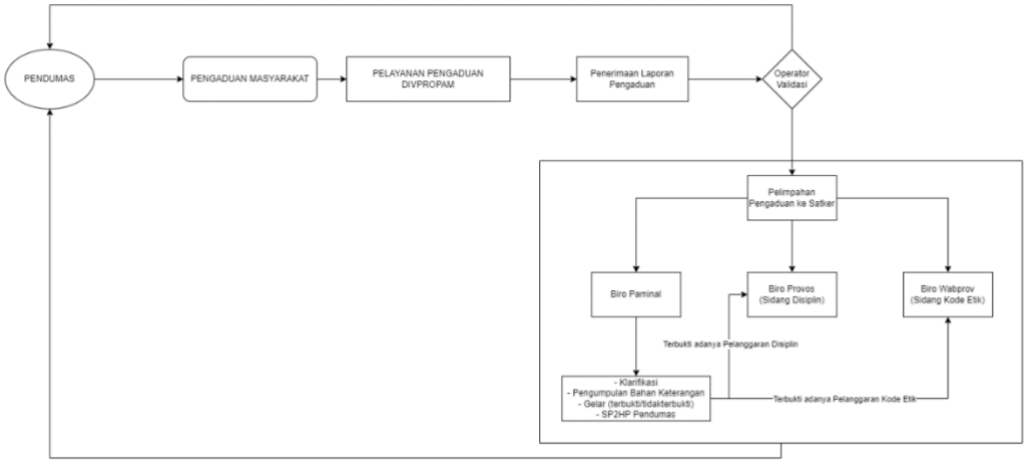


Figure 3.National Police DMS Workflow

A Database Management System is a computerized system whose main objective is to maintain and provide access to information. Composed of the following elements, the Database System functions as an integrated data file preparation system:

1. *Database* (Database)
2. *Software (Software)*
3. *Hardware (Hardware)*
4. *Brainware* (Human)

Benefits of Police DMS:

1. Integrated between bureaus and departments
2. Integrated between the center and regions/polda
3. Realtime
4. Dumas monitoring system
5. There is no duplication of handling
6. There is an integrated service center
7. Realizing fast, easy, transparent and accountable services

DMS has a multi-layered security system. Each layer/layer has its own security. This security includes network security (transport), hardware (physical), operating system, firewall (door), database (data/content), best practice (backup management). In the transport (network) layer ; DMS places the server in DIV TI as an outer firewall. Threats must be able to penetrate the DIV IT network security first before they can attempt to penetrate DMS security. DMS uses HTTPS which is encrypted from end to end (end to end encryption) DMS activates firewalls and threat management to read and examine incoming and outgoing data traffic on the network.

At the Hardware (physical) layer: DMS uses a branded dedicated server from a clear brand. Ensure physical server security standards that do not have backdoors. Maximum security from all physical threats such as dust, moisture, static electricity and others

Operating System: DMS uses Windows Server 2019 which is the latest operating system product from Microsoft with all the advantages of security and stability to be active 24x7. Firewall Layer: DMS implements an outer and inner firewall. The outer firewall is controlled and secured by the DIV TI firewall while the inner firewall is guarded by a firewall system that is active from the window server. All ports/doors are closed except for web access using strict encryption and passwords.

Data layer: DMS uses ORACLE 18 C. ORACLE is the largest database producer in the world which is commonly used by world-class corporations and banks. It is well known for its stability and data security. DMS was built from the start with awareness about computer and data security.

The system is built without using templates or frameworks (templates/frameworks will speed up development but will sacrifice security)

For data security, it is always backed up every midnight and every weekend.

The above is in line with the National Police Chief's Priority Program (PPK) 2021 – 2024, which in total includes 16 Priority Programs, one of which is the modernization of modern police technology in the Police 4.0 era (PPK 4). A description of the activities included in this program are: unification of an integrated police information system, fulfillment of police facilities and infrastructure, and making the National Police Research and Development Center a police technology research center. The urgency of using information technology in carrying out the duties of the National Police is very urgent, therefore PPK 4 should really be implemented by the National Police institution.

CONCLUSION

Based on the discussion above, it can be concluded that the Indonesian police strategy in improving public services to the community is related to the unprofessionalism of Indonesian police members, strengthened by using the Indonesian police database management system. This system saves data that has been stored in old filling & recoding applications. Developing new applications that are integrated with each bureau and can be accessed by all regional police to regional police. The focus of the research that will be carried out by researchers, which is different from previous researchers, lies in an in-depth study of the number of alleged abuses of authority committed by members of the National Police and the number of unprofessionalism in the positions they are currently holding through the National Police Divpropam Management System Database. Then, from the results of this study, researchers will try to formulate a model for strengthening accountable and transparent performance as an effort to increase public trust in society

BIBLIOGRAPHY

AB Whinston, Clyde Holsapple. 2012. *Database Management: Theory and Applications* . Publisher: Springer Netherlands

Abidin, Said Zainal. 2004. *Public Policy* . Jakarta: Pancur Siwah Foundation.

Anwar, Dessy, 2001, *Complete Indonesian Dictionary* , Jakarta, Abditama's work.

Alshawi, M. & Ingirige, Bingunath. 2003 . *Web-enabled Project Management: An Emerging Paradigm in Construction.* Journal of Elsevier Science, Automation in Construction. Vol. 2, p. 56

Bocij. et al. 2003. Business Information Systems Technology, Development and Management for E-Business. Second Edition, Prentice Hall, London.

Bromley, Daniel W. 1989. *Economic Interest and Institutions: The Conceptual Foundations of Public Policy* . New York: Basil Blackwell.

Caballero, A. (2014). *Information security essentials for IT managers: Protecting mission-critical systems.* In J. Vacca (Ed.), Managing information security, 2nd ed., pp. 1–45 Elsevier Inc.

Cangara. 2008. *Introduction to Communication Science* (2nd edition), Rajawali Press, Jakarta.

Chaeikar, S., Jafari, M., Taherdoost, H. and Chaei Kar, N. (2012). *Definitions and criteria of CIA security triangle in electronic voting system. International Journal of Advanced Computer Science and Information Technology* , 1(1), 14–24.

Cherdantseva, Y., & Hilton, J. (2013). *A Reference Model of Information Assurance & Security. In 2013 International Conference on Availability, Reliability and Security* (pp. 546–555). IEEE. https://doi.org/10.1109/ARES.2013.72

Chassiakos, A.P. & Sakellaropoulos. 2008. *A Web-based System for Managing Construction Information* . Journal of Elsevier Science, Advances in Engineering Software. Vol. 1, p. 98

Daft, Richard L. 2007. " *Management" (Translation) Sixth Edition, Book One* . Jakarta: Salemba Empat Publishers.

Damar, AS (2018). *Strategy of the National Cyber and Crypto Agency (BSSN) in Facing Cyber Threats in Indonesia* . University of Indonesia: SKSG UI.

Dainty, Andrew at all. 2006. *Communication in Construction* . UK: Taylor & Francis.

Dallaire, Rene M. 1992. Data-Based Marketing for Competitive Advantage Information Strategy. The Executive's Journal, Vol 8.No.3.

Daniels, D. Tom, Barry K. Spiker, and Michael Papa (1997). *Perspectives on Organizational Communication* , 4 th edition, Boston, MA: McGraw Hill.

Date, C.J., *An Introduction to Database Systems* (8th Edition). Pearson Education Inc. United States of America.

Dunn, William N,. 2000. *Public Policy Analysis.* Gadjah Mada University Press, Yogyakarta.

Dhawan, S. (2014). *Information and data security concepts, integrations, limitations and future. International Journal of Advanced Information Science and Technology* , 3(9), 1–5.

Dwijowijoto, Riant Nugroho, 2004. *Public Policy. Jakarta: Elex Media Komputindo*

Dwilaksana Chryshnanda, 2004, Kohan and chuzaicho, 6th edition of the Indonesian police journal, Jakarta, Foundation for the Development of Police Science Studies.

_____, 2009, Life Guard Police, Jakarta, Foundation for the Development of Police Science Studies.

_____, 2009, Becoming a Conscientious Police Officer, Jakarta, Foundation for the Development of Police Science Studies.

_____, 2002, Problems of Indonesian police reform, Jakarta, Trio repro. More, 1998, special topics in Policing, Cincinnati , Andreson Publishing. Rahardjo, Satjipto, 2002, Civil Police, Jakarta, Gramedia

_____, 2000, The Figure of the People's Police Towards a New Indonesia,

Dye, Thomas R. 1992. *Understanding Public Policy Analysis: An Introduction, Second Edition* (translation). Yogyakarta: Publisher Gadjah Mada University Press.

Edward III, George C. 1980. *Implementing Public Policy* . Washington DC : Congressional Quarterly Inc.

Fauzi, Ahmad (1997). *Main Focus of Management Information Systems in Improving Schedule Performance on Multi-Storey Building Construction Projects* in Jakarta. Thesis, Faculty of Engineering, University of Indonesia.

Fruhlinger, Josh. 2020. *The CIA triad: Definition, components and examples* . US: Foundry

Georgopoulos and Tannenbaum AS 1957. *Critical Issues in Assessing Organizational Effectiveness* , American Sociological Review, Gerson, RF

Gie, The Liang. 1967. *Prospects for Regional Autonomy in the Republic of Indonesia* , Jakarta: PT. Raja Grafindo Persada, 1967 and The Liang Gie, Modern Office Administration, Yogyakarta: Supersukses and Nur Cahaya, 1988.

Haubinger, F. (2015). Studies on employee information security awareness [Doctoral thesis, Georg-August-Universität Göttingen]. https://ediss.uni-goettingen.de/handle/11858/00-1735-0000-0022-6021-8

Handayaningrat, Soewarno. 1994. *Government Administration in National Development* , Jakarta: Mas Agung.

Hansen, L & Nissenbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School.* International Studies Quarterly, Vol. 53, no. 4.

Hardiyansyah. 2012. *Public Sector Human Resources Administration and Management System* , Yogyakarta, Gava Media.

Hidayat. 1986. *Effectiveness Theory in Employee Performance,* Gajah Mada University Press, Yogyakarta.

Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Howlett, Mitchell and M. Ramesh. 1995. *Studying Public Policy: Policy Cycles and Policy Subsystems.* Oxford: Oxford University Press.

Islamy, Irfan. 1994. *Principles of State Policy Formulation* , Jakarta: Bumi Aksara.

James. 2002. Information *Technology for Management Making Connections for Strategic Advantage.* 3rd Edition. John Wiley & Sons Inc.

K. Kim, ME Aminanto and HC Tanuwidjaja. 2018. Network Intrusion Detection Using Deep Learning : A Feature Learning Approach, Singapore: SpringerBriefs in CyberSecurity Systems and Networks.

Kurniawan, Agung. 2005. *Transformation of Public Services* , Yogyakarta: Update.

Kozier, B.J., Erb, G., Berman, A.J., & Snyder, S. (2011). *Nursing Fundamentals Textbook: Concepts* , Process & Practice (7 Vol 1). Jakarta, Indonesia: EGC.

Lawler, EE 2003. *Reward Practices and Performance Management System Effectiveness* . Center for Effective Organizations.

Laudon. 2002. Management Information Systems. Seventh Edition. Prentice Hall.

Lee, Seul-Ki & Yu, Jung-Ho. 2012. *Success Model of Project Management Information System in Construction. Journal of Elsevier Science* , Automation in Construction, p. 83

Lee, R. M. (2015). *The Sliding Scale of Cyber Security* . SANS Reading Room. https://www.sans.org/reading-room/whitepapers/ActiveDefense/slidingscale-cyber-security-36240

Li, Ji at all. 2006. *Internet-based Database Management System For Project Control. Journal of Emerald, Engineering* , Construction and Architectural Management.

Lubis, Hari. SB and Martani Huseini. 1987. *Organization Theory (A Macro Approach)* , Inter-University Center for Social Sciences, University of Indonesia, Jakarta.

Nitham Young, P. & Skibinski, Miroslaw J. 2004. *Web-based Construction Project Management Systems: How to Make Them Successful?.* Journal of Elsevier Science, Automation in Construction. Vol. 3, p. 77

Marquis & Huston. 2010. *Nursing leadership and management. Theory and application.* Edition 4. (Widyawati et al, Translator). Jakarta: EGC

Merriam-Webster. (2019). Definition of CYBERSECURITY. https://www.merriam-webster.com/dictionary/cybersecurity

McLeod, Raymond. 2001. *Management Information Systems* . 7th Edition. New Jersey: Prentice Hall, Inc.

Meliala, Adrianus, 1999. *Collection of writings before and after the Police left Abri* , University of Indonesia.

_____, 2002, Criticizing the Police, Yogyakarta, Kanisius.

Mondy, R. Wayne., Noe, Robert M. & Premeaux, Shane R. 2002. " *Human Resource Management* " 8th Edition. New Jersey : Prentice Hall.

MS Othman, FM Ba-Alwi, N. Alsohybe and AY Al-Hashida. 2018. "Intrusion Detection Model Using Machine Learning Algorithm on Big Data Environment," Journal of Big Data, vol. 5, no. 34.

Muhammad, DR. Farouk, and Prof. DR. H. Djaali, *Social Research Methodology,* PTIK Press CV. Restu Agung, Jakarta 2003, p. 35.

Mustopadidjaja, AR 1998. *Developments in the Application of Policy Studies* . Jakarta : LAN.

Nawawi, H Hadari. 2000. " *HR Management" 3rd Print.* Yogyakarta : Gamma.

Nugroho, Riant. 2009. *Public Policy* . Jakarta: PT Elex Media Komputindo

Noe, R.A., Hollenbeck, J.R., Gerhart, B., & Wright, P.M. 2015. *Human Resource Management: Gaining a competitive advantage,* 9e. Global Edition. Berkshire: McGraw-Hill Education.

Niti Baskara, TB Ronny, 2000. *Improving Morality as a Prerequisite for Changes in Police Performance & Behavior* , Workshop Paper at PTIK 29 February 2000.

Nugroho, Riant. 2009. *Public Policy* . Jakarta: PT Elex Media Komputindo

O'Brien, J.A. 2001. "Introduction to Information Systems Essentials for the Internet Worked E Business Enterprise. Tenth Edition. McGraw-Hill.

Parsons, Wayne. 2005. *Public Policy Introduction to the Theory and Practice of Policy Analysis* . Jakarta : Kencana.

P. Mishra, V. Varadharajan, U. Tupakula and ES Pilli. 2019. "A Detailed Investigation and Analysis of Using Machine learning Techniques for Intrusion Detection," IEEE Communication Surveys and Tutorials, vol. 21, no. Number 1.

Porter. 1985. Competitive Advantage: Creating and Sustaining Superior Performance, Free Press.

Post and Andersen.2000. Management Information System Solving Business Problems with Information Technology. Second Edition. McGraw Hill, USA.

Rahardjo, Satjipto, 1998. *Re-examining the Role and Function of the Police in Society in the Reform Era* , National Seminar paper on Police and Society in the Reform Era

———————, 2002. *Civil Police* , Jakarta, Gramedia.

———————, 2001. *About Community Policing in Indonesia* , Seminar paper "Police between hope and reality", Borobudur Hotel, Jakarta.

Randeree, E. (2006). Knowledge management: Securing the future. Journal of Knowledge Management, 10(4), 145–156. https://doi.org/10.1108/13673270610679435

Rasdiyanah. 2017. *The Effect of Health Education Using Booklet and Diary Media on the Self-Efficacy and Motivation of Housewives with Hypertension in Depok City* . University of Indonesia.

Ramelan, Rahadi. 1999. *Increasing National Productivity Through Mastery of Science and Technology and Human Resource Development.* University of Indonesia, Jakarta

Robbins & Coulter. 2002. *Management (activebook*), 7/e. Stephen P. Robbins and Mary Coulter. New Jersey: Prentice Hall. Inc. http://sirpabs.ilahas.com/Management, Robbins-CoulterStudentEd.29.pdf

Robert, Roy R and Jack Kuykendall. 2012. *Police Management.* Jakarta, PTIK Press.

Richard M. Steers. 1985. *Organizational Effectiveness (Rules of Behavior).* Jakarta: Erlangga.

Samonas, S., & Coss, D. (2014). *The CIA strikes back: Redefining confidentiality, integrity and availability in security* . Journal of Information Systems Security, 10, pp. 21–45.

Sedarmayanti . 2007. *Human Resources Management, Bureaucratic Reform and Civil Servant Management.* Refika Aditama, Bandung

Singh.A.2004. Trends in South African Internet Banking. Aslib Proceedings: New Information Perspectives. Volume 56.No.3.

Snell, SA, Morris, SS, & Bohlander, GW 2016. *Managing Human Resources* . Boston: Cengage Learning.

Suleiman A. Al Khatttab, 2005. The Impact of Information Technology on Customer Service in The Jordanian Banking Sector", A Thesis Submitted in Partial Fulfillment of the Requirements of the University of Salford for the degree of Doctor of Philosophy, University of Salford

Suarli & Bahtiar. 2010. *Nursing management with a practical approach.* Jakarta: Erlangga Publishers.

Suharto, Edi. 2006. *Public Policy Analysis: A Practical Guide to Examining Social Problems and Policies* . Bandung: Alphabeta.

Soewarno Handayaningrat S. 1994. *Introduction to the Study of Administration and Management Science* . Jakarta: Masagung Hajj.

Swansburg, CR 2000. *Nursing leadership & management for clinical nurses* (Suharyati Samba, Translator). Jakarta: EGC.

Turban. et al. 1996. Information Technology for Management Improving Quality and Productivity. John Wiley and sons, Inc.

Wahab, SA 2008. *Policy Analysis: From Formulation to Implementation of* State Policy. Jakarta : Earth of Letters

Whitman, M., & Mattord, H. (2011). Management of information security (3rd ed). Thomson Publishing.

Walt and Gilson, 1994, *Policy Analysis Triangle.*

Wibowo. 2010. *Performance Management* (Third Edition). Jakarta : PT. Rajawali Press.

Wiryanto. 2004. Introduction to Communication Science. Jakarta: PT Gramedia Widiasarana Indonesia

Wiscombe, Janet . 2000. *Can Pay for Performance Really Work? Workforce* 80, no. 8.

Y. Zhou, G. Cheng, S. Jiang and M. Dai. 2020. Building An Efficient Intrusion Detection System Based On Feature Selection and Ensemble Classifier, computer Networks, vol. 174

Yuniarsih T & Suwatno. 2009. *Human Resource Management, Theory, Applications and Research Issues* , CV. Alphabeta, Bandung

Zwick, D., & Dholakia, N. (2004). Whose identity is it anyway? Consumer representation in the age of database marketing. Journal of Macromarketing, 24(1), 31–43. https://doi.org/10.1177/0276146704263920