www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Maturity Level Analysis of Digital Evidence Handling on Integrated Criminal Justice System based on NIST SP800-53 Revision 5 Using NIST Maturity

Chandra Tirta Aditya Gunawan[1], Yohan Suryanto[2]
[1,2]*Information and Network Security Management, Electrical Engineering, Universitas Indonesia*
Chandra.tirta@ui.ac.id, yohansuryanto@ui.ac.id

Abstract

The challenge of handling digital evidence in an integrated justice system is that it is vulnerable, easy to change, and destroyed, so it needs to be protected from security threats when stored, processed, and transmitted by each interconnected law enforcer. This study aims planning evaluation as a part to enhance security control by analyzing the maturity level of XYZ's organization as a law enforcement in handling digital evidence in an integrated criminal justice system. So far, there has been no research that measures the level of maturity in the handling of potential digital evidence. This study uses the NIST SP800-53 Rev 5 security control standard and measures the maturity level using NIST Maturity. The result of the research is that the current organizational maturity level is 2.1 (range 0-5). The XYZ organization, in general, has had a pattern in dealing with digital potential in terms of information security and privacy, but it has not been established so it is still vulnerable, inconsistent, and reactive. Organizations need to improve control of information security and privacy optimally so that the security of digital evidence can be guaranteed. These results can be part of the evaluation process of the organization's planning to improve security controls.

Keywords
integrated criminal justice system; digital evidence; maturity level; NIST SP 800-53 Rev 5; NIST maturity

I. Introduction

Integrated Criminal Justice System in Indonesia based on the Criminal Procedure Code (KUHAP) that contains three outlines of the stages of examining criminal cases, namely the investigation stage, the prosecution stage, and the examination stage in court. The authority of investigator, prosecutor, and judge is carried out separately by each law enforcement agency, even though they are a unified whole or interrelated. (Supriyatna 2009) (Dananjaya 2014) A judge may not impose a sentence on a person except with at least two valid pieces of evidence. Legal evidence is the testimony of witnesses, expert opinion, letters, instructions, and statements of the defendant ("Constitution of Indonesia 8/1981 about Criminal Procedure Law" 1981). Along with the development of information technology, it has a significant impact on the law in Indonesia. One of them is the recognition of the existence of electronic evidence in the evidence in court as regulated in Article 26A of Constitution of Indonesia no. 20 of 2001, concerning Amendments to Constitution of Indonesia no. 31 of 1999 concerning the Eradication of Criminal Acts of Corruption and Constitution of Indonesia no. 11 of 2008, concerning Information and Electronic Transactions which expands the scope of evidence in the Criminal Procedure Code, including digital evidence ("Constitution of Indonesia 11/2008 about Information and Electronic Transactions" 2008; "Constitution of Indonesia 20/2001 about Eradication of Corruption" 2001).

Potential digital evidence is data needed to prove a crime that occurred in court. Digital evidence is stored and transmitted through a digital device, network, or communication system, not a physical form of the electronic device. ("ISO/IEC 27037:2012 Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence" 2012) (Anderson and European Union. European Network and Information Security Agency. 2014; Mukasey et al. 2001). Digital evidence has three basic principles, namely firstly relevance, digital evidence is potentially relevant when it has relevance to the particular case being investigated (Feri Efendi et al. 2020). Second, reliability, every step is taken in handling potential digital evidence must be auditable and repeatable. Third, the adequacy of the data collected is sufficient for the investigation process (Prayudi 2014). These three principles are necessary to the investigative process, not limited to the evidence in court.

In the law enforcement process, it is very important to carefully evaluate the quality and authenticity of the evidence to avoid wrong decisions (Arshad et al. 2018). However, the challenge in managing potential digital evidence is that it is vulnerable, which means it is easy to change, manipulate, and destroy (Prayudi 2014). The potential digital evidence needs to be protected from information security threats as it is processed, stored, and transmitted by third-party (Tian et al. 2019), in this case, affiliated law enforcement agencies. Measurable special handling is important to maintain the security of potential digital evidence, data integrity, and chain of custody in an integrated criminal justice system so that potential digital evidence can be used to prove a crime. To improve information security control, the first step that can be taken by the organization is to measure the maturity level. But so far, there has been no research that measures the maturity level of handling potential digital evidence. So that organizations find it challenging to map out the suitability of handling potential digital evidence with applicable security control standards and provide an overview of the organization's readiness to carry out security clauses and controls according to their needs.

The measurement of the level of security analysis has previously been carried out by Rosmiati, et al. conducted a study to determine the level of information security in the organization to provide recommendations for improvement using all the clauses contained in ISO 27001 for improvements. (R et al. 2016). Kurniawan researched to determine the level of information security in the organization and provided recommendations for improving information security management using all the clauses contained in ISO 27002 (Kurniawan and Riadi 2018). Pradana conducted a study to identify the level of impact of information that will be mapped on NIST SP800-53 on the XYZ organization as a benchmark to comply with regulations in Indonesia in managing personal data through the implementation of internal policies. The results of privacy controls can be a recommendation for improvement in the formulation of personal data protection at the XYZ organization (Yoga Pradana and Trianto 2018). Avianto and Ogi conducted an analysis and risk assessment of ESDM management at SIMRS hospitals. Mapping security and privacy controls based on NIST SP800-53 Rev 5 as an option for hospitals to improve ESDM on SIMRS (Avianto and Ogi 2019).

This study uses the NIST SP800-53 Rev 5 security control standard as one of the international references in the security standards. NIST SP800-53 Rev 5 has security and privacy controls that organizations can use to define rules according to organizational needs. The selection of rules can be adjusted to the organization's business processes, the requirements of the legislation in which this research is structured according to the integrated criminal justice system based on the Criminal Procedure Code, and security threats. The NIST Maturity tool is used to measure the maturity level.

The purpose of this study is to measure the level of organizational maturity in handling digital evidence through the examination process. Checking the information security control clause with NIST SP800-53 Rev 5 which has been adapted to the needs of the organization. The process begins with compiling security and privacy controls by business processes in handling digital evidence in an integrated criminal justice system using NIST SP 800-53 Rev 5. Next, analyze the security and privacy maturity level of the organization using NIST Maturity, obtain measurement results, analyze measurement results as the basis for improving control clauses to organizations to improve information security control management in handling digital evidence.

II. Review of Literature

2.1 Digital Evidence in Law Enforcement Process

According to Article 184 of the Criminal Procedure Code, valid evidence is witness testimony, expert testimony, letters, instructions, and statements from the defendant. The function of digital evidence is to be analyzed by experts and form expert statements which are legal evidence that can prove the occurrence of a crime. Expert testimony is presented under oath before a panel of judges in court ("Constitution of Indonesia 8/1981 about Criminal Procedure Law" 1981). A certain case in proving corruption cases, the position of digital evidence is as evidence. In particular, the Criminal Procedure Code does not regulate digital evidence, but Constitution of Indonesia no. 11 of 2008 concerning Information and Electronic Transactions and Constitution of Indonesia no. 20 of 2001 concerning the Eradication of Criminal Acts of Corruption, concerning digital evidence in proving corruption in a lex specialist manner. Article 26A of the Constitution of Indonesia no. 20 of 2001, expands the scope of evidence guided by the Criminal Procedure Code. (Nugroho 2010)

The process of searching and collecting digital evidence begins at the investigation stage. Investigators and prosecutors are looking for digital evidence related to criminal acts. Investigators have the power to make coercive efforts to collect additional digital evidence by search and seizure. A search is an investigator's effort to search for potential digital evidence related to non-crime. Confiscation is a series of actions by an investigator to take over and or keep under his control movable or immovable, tangible or intangible objects for proof in the investigation, prosecution and court. The confiscated objects before being wrapped, are recorded in their weight and/or amount according to their respective types, characteristics and characteristics, place, day and date of confiscation, the identity of the person from whom the objects were confiscated, and others which are then given a note and signed by the investigator (Article 130 of the Criminal Procedure Code).

In this process, investigators and prosecutors are assisted by a Digital Evidence First Responder (DEFR) and a Digital Evidence Specialist (DES) to carry out the identification, collection, and acquisition of potential digital evidence ("ISO/IEC 27037:2012 Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence" 2012). The potential digital evidence is then analyzed for its relevance to the crime by the investigator and can be assisted by an expert appointed by the investigator. If the investigator or public prosecutor believes that the confiscated object is no longer needed for proof, it can be returned to its owner.

The completion of the investigation process is marked by the title of the case and the submission of files and digital evidence to the public prosecutor, which will then be proven in court. After the evidence and decision of the panel of judges in court, the panel of judges can consider the status of the accused and the follow-up of the evidence. Judges can

provide recommendations for storing digital evidence data related to criminal acts as well as deleting and returning potential digital evidence data that are considered not related to criminal acts. The process is further explained through a flowchart as follows:

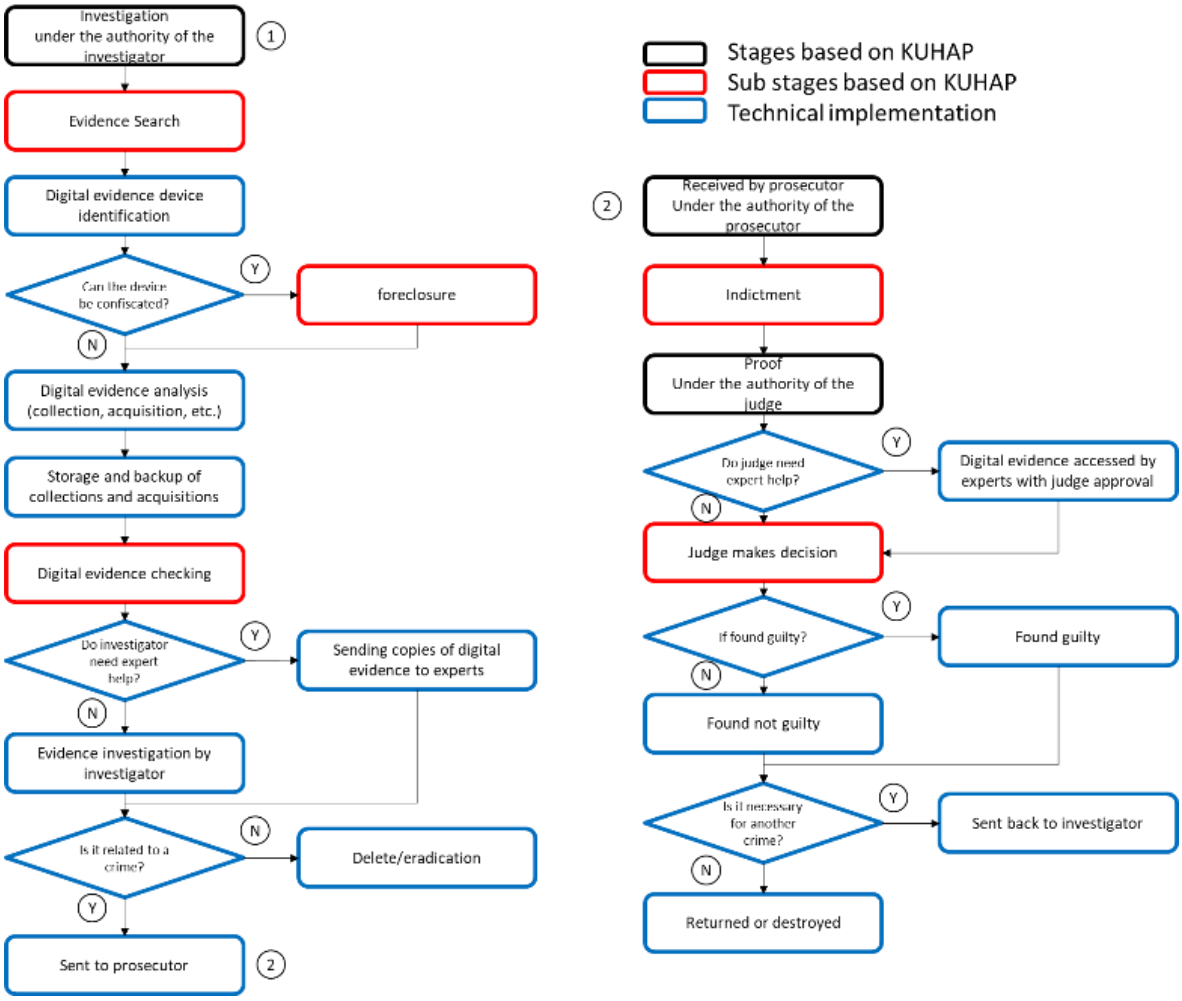

Figure 1. *Integrated Criminal Justice System*

2.2 NIST SP800-53 Revision 5

Security control is a protective measure implemented by the organization to protect the confidentiality, integrity, and availability as a parts of information security. Meanwhile, privacy control is an administrative, technical and physical security measure implemented by an organization to manage privacy risks and to provide the organization's compliance with applicable privacy provisions ("NIST SP800-53 Revision 5 - Security and Privacy Controls for Information Systems and Organizations" 2020). Both are selected and implemented by the organization according to its needs to meet security and privacy requirements based on laws and regulations, government regulations, standards, policies, management directives, and organizational requirements to ensure the confidentiality, integrity, and availability of information by the organization against individual privacy risks. All of these characteristics are found in the NIST SP800-53 Rev 5.

NIST SP 800-53 has historically served as the basis for security controls used by the US government and has been widely adopted in the healthcare sector and other critical infrastructure and private sector organizations. NIST SP800-53 has a companion document, NIST SP800-53a, which details each security control and outlines the

procedures applicable to assessing the commands established to ensure the effectiveness of security controls. The most significant additions to the controls sit in third-party risk controls, supply chain, privacy, and new areas such as cyber resilience, secure systems design, and governance models. This is prepared so that NIST SP800-53 Revision 5 can be applied to a wider organizational scale, and a variety of systems, not only specific to federal information systems ("NIST SP800-53 Revision 5 - Security and Privacy Controls for Information Systems and Organizations" 2020).

An organization's essential task is to select, design and implement its security and privacy controls to protect the business processes and assets of the organization as well as the well-being of individuals and nations. The task has significant implications for the smooth running of organizational goals. Previously, organizations must ensure the security and privacy controls needed to adequately manage and deal with risks, plan the implementation of security controls, and aspects required for organizations to measure the effectiveness of the implemented controls. NIST SP800-53 Rev 5 is an appropriate control to be used as a reference in this study.

2.3 Maturity Model

The security maturity model was chosen because it can help to better manage organizational security, enable better security risk management processes, save costs, improve organizational governance, and support good security procedures and processes. In addition, it can help prevent organizations from applying controls blindly without regard to organizational conditions (Le and Hoang 2016). Organization must have a goal to be achieved by the organizational members (Niati et al., 2021).

In this topic, the organization can evaluate itself from level 0 (lowest) to level 5 (highest). 0 – Non-Existing, organizations do not care about the importance of information security and privacy; 1 – Initial, organizations apply security and privacy controls reactively, without prior planning. The status are reactive, inconsistent, high risk; 2 – repeatable, the organization already has a recurring pattern in activities related to information management and privacy, but it is not well defined. The status are inconsistent, volatile, manual; 3 – defined, the organization already has information security and privacy controls that have been socialized to all employees; 4 – quantitively managed, the organization already has security controls maintained, reviewed, and developed regularly; and 5 – optimizing, the organization already has information security and privacy controls that have been referred to as "best practice". Organizations can determine the extent to which they meet information security standards and can use an identification framework that is represented in maturity levels. The results of the organizational maturity assessment will show how the organization carries out its business processes. Next, it is necessary to determine the ideal corporate maturity target for each function, which becomes a reference in the security management model that the organization wants to develop. The gap between the current organizational maturity level and the predetermined organizational maturity target will be analyzed for optimization (Chiper 2020). This tool can also be used to measure organizational governance, understand how well the organization identifies threats, find out if the organization can protect itself from threats, and assess overall response capabilities.

2.4 Gap Analysis

Gap analysis is one of the most important tools used for performance evaluation both during planning and evaluation. This method is the most commonly used in managing the organization's internal management. In general, "gap" represents the difference between

one thing and another. In the purpose of evaluating, the gap describes the difference between the actual conditions in the organization and the ideal conditions to be achieved. The smaller the gap, the better the quality of organizational performance (Kohar et al. 2015).

III. Research Method

Research methodology can be seen in table 1 below:

Table 1. Research Methodology

Phase	*Process*
Preparation	Problem identification
	Define goals
	Literature Review
Maturity tool design	Setting objective clauses based on business processes
	Identification and classification security control clauses standards NIST SP800-53 Rev 5.
	Setting control clauses based on objective clauses using the international standard NIST SP800-53 Rev 5 on security and privacy controls
Data collecting and analysis	Creates a questionnaire based on the control clause to renspondents at the XYZ organization about the existing condition in the organization using a control clauses that has been prepared.
	Measuring the level of organizational maturity against the control clause using NIST Maturity.
	Analyze the maturity level and calculate the gap analysis of organizational maturity with the intended ideal conditions.
Result	Conclusion and recommendation

The limitation of the problem in this research is that it is only carried out in the Integrated Criminal Justice System based on the Criminal Procedure Code (KUHAP). Information security and privacy control management is applied to potential digital evidence that has been identified to the criminal act, and includes electronic devices suspected of storing potential digital evidence. The research site is the XYZ organization as a law enforcement agency.

IV. Results and Discussion

4.1 Control Design

NIST SP 800-53 Rev 5 has 20 control clauses that allow the organization to apply controls according to the conditions of the organization. At this stage, the authors analyze the clauses contained in the NIST SP 800-53 Rev 5 standard and their application to the control aspects of information security and privacy. It is designed to create protection and privacy controls that match the business processes required by the organization. The combination of security and privacy controls and the selection process of risk-based controls on business processes can help organizations comply with security and privacy requirements, obtain adequate protection for their information systems, and protect individual privacy. Table 2 below is a codification of the stages and sub-stages of the integrated criminal justice system.

Table 2. Subject Code

CODE	SUBJECT	CODE	SUBJECT
DIK	Investigation	DIK.AD	Digital analysis
TUT	Prosecution	DIK.PD	Digital evidence checking
DIL	Court	TUT.PT	Prosecution
DIK.PP	Searches and confiscations	DIL.PB	Proof
		DIL.PT	Judge's decision

The description of the business processes of each stage based on the integrated criminal justice system can be seen in table 3.

Table 3. Business Process Based on Integrated Criminal Justice System

Stages	Sub-stages	Description
DIK	DIK.PP	The process of searching and retrieving electronic devices suspected of containing potential digital evidence. In this sub-stage, there is a process of identifying data, sending data, and documentation.
	DIK.AD	The process of identification, collection, and acquisition of digital evidence from parties related to criminal acts. In addition, there is a process of sending data from DEFR and DES to investigators, data storage, data backup, and documentation.
	DIK.PD	The process of analyzing the relationship between digital evidence and alleged criminal acts that occurred. In this sub-stage, there is a process of sending data between investigators and expert witnesses and public prosecutors, data preservation, and data eradication if the data is deemed irrelevant to the alleged crime.
TUT	TUT.PT	The public prosecutor received a case file from the investigator in the form of a suspect and digital evidence which was then used as the basis for the charge. In this process contains identifying and sending data.
DIL	DIL.PB	The process of proving the link of potential digital evidence with the alleged crime that occurred is carried out before the panel of judges at trial, the judge has the authority to invite independent experts. In this sub-stage, there is the process of sending data and preservation.
	DIL.PT	The decision is decided by the panel of judges based on the available evidence. The judges gave recommendations to keep or reuse the evidence for other cases, return or delete the digital data. In this sub-stage, there are processes of sending data, returning data, deleting data, and documentation.

The objective of control based on business processes on the handling of digital evidence in an integrated justice system can be seen in table 4.

Table 4. Objective Controls

Code	Objective	Description
DTR	Data transfer	In an integrated criminal justice system, law enforcers at the investigation, prosecution and judicial stages act as a unified whole and are related to each other. A process for controlling data transmission is required, in order to maintain the security

		of the data.
DST	Data storage	Potential digital evidence that has been confiscated for inspection purposes needs to be appropriately stored and safeguarded, so adequate controls are required to store data.
DBU	Data backup	Potential digital evidence has vulnerable characteristics, so it is essential to back up data to anticipate damage or loss.
DOC	Documentation	The documentation process is needed to ensure that every step taken by law enforcement in handling potential digital evidence is documented and ensures the chain of custody and data integrity.
DIC	Data Identification and classification	The identification and classification process is needed to classify potential digital evidence data according to their characteristics so that they can be handled properly and prevented from damage.
CLA	Collection and acquisition	The collection and acquisition process is taken out by law enforcement in seizing potential digital evidence.
DRT	Data return	If the potential digital evidence confiscated by law enforcement is not related to a criminal act, it can be returned with a secure data return mechanism.
DER	Data eradication	If the potential digital evidence is confiscated by law enforcement, information data and systems are no longer operated by the institution, it can be deleted with appropriate controls.

Furthermore, based on the needs of the objectives that have been prepared, determine the controls contained in the NIST SP800-53 Revision 5 clause, listed in table 5.

Table 5. Control Clause Based on NIST SP800-53 Revision 5

No	Objective	Control
1	DTR	MP-2 Media Access, MP-5 Media Transport, SC-8 Transmission Confidentiality and Integrity, SC-11 Trusted Path, PE-16 Delivery and Removal, PE-20 Asset Monitoring and Tracking, AC-4 Information Flow Enforcement, AC-21 Information Sharing, PE-4 Access Control for Transmission, PE-5 Access Control for Output Devices
2	DST	SC-28 Protection of Information at Rest, AU-4 Audit Log Storage Capacity CP-10 System Recovery and Reconstitution, PE-2 Physical Access Authorizations, PE-3 Physical Access Control, PE-8 Visitor Access Records MP-4 Media Storage
3	DBU	SC-28 Protection of Information at Rest, CP-6 Alternate Storage Site, CP-9 System Backup
4	DOC	SA-5 System Documentation, CM-3 Configuration Change Control
5	DIC	MP-7 Media Use, SI-10 Information Input Validation, MP-3 Media Marking
6	CLA	MP-4 Media Storage, MP-5 Media Transport, MP-7 Media Use
7	DRT	MP-1 Policy and Procedures
8	DER	MP-6 Media Sanitization

Based on the description of business processes in table 2 and control categories in table 3, a list of the implementation of information security and privacy controls can be seen in table 6.

Table 6. Control Implementation Based on Business Process

Stages	Sub-stages	DTR	DST	DBU	DOC	DIC	CLA	DRT	DER
DIK	DIK.PP	■			■	■	■		
	DIK.AD	■	■	■	■	■	■		
	DIK.PD	■							■
TUT	TUT.PT	■				■			
DIL	DIL.PB	■							
	DIL.PT	■			■			■	■

Note: Applied controls are marked with a green column.

4.2 Maturity Level Analysis

Assessment is carried out on each control clause contained in each predetermined objective clause.

Table 7. Maturity Level of Data Transfer

Objective	**NIST SP800-53 Rev 5 Control**	**Value**
(DTR) Data transfer	MP-2	2
	MP-5	2
	SC-8	2
	SC-11	3
	PE-16	3
	PE-20	1
	AC-4	2
	AC-21	2
	PE-4	2
	PE-5	3

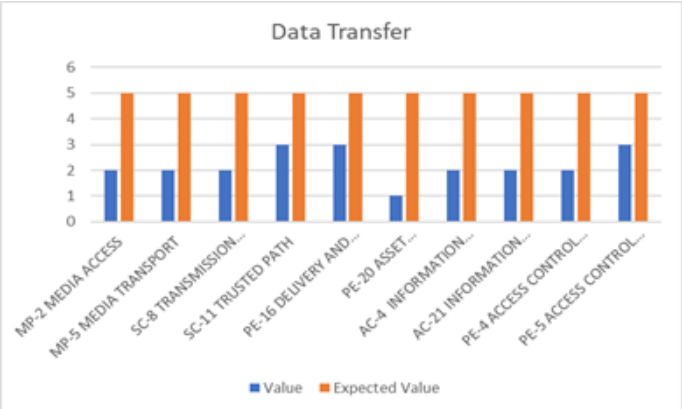

Figure 2. *Maturity Level of Data Transfer*

Table 7 and figure 2, show the results of measuring the maturity level for the objective of transfer data. The organization has properly documented SC-11, PE-16, and PE-5 control clauses (level 3 – defined). This shows that the organization already has a trusted communication line for users for data transmission, enforces entry and exit

authorization in the data storage system and access to the delivery area, implements physical access control to output devices in a secure location, and is monitored by personnel. Even though the organization needs to improve it to reach level 5 – optimizing. Furthermore, there is one of the lowest measurement values (level 1 – initial) in the PE-20 control clause. Organizations still apply control reactively, without prior planning. This results in the transfer of digital evidence not being recorded and properly monitored, which can lead to confidentiality vulnerabilities. In addition to the controlling clause, the organization has started to carry out control with a repetitive pattern even though it has not been appropriately documented and implemented (level 2 – repeatable).

Table 8. Maturity Level of Data Storage

Objective	**NIST SP800-53 Rev 5 Control**	**Value**
(DST) Data storage	SC-28	3
	AU-4	2
	CP-10	1
	PE-2	3
	PE-3	3
	PE-8	2
	MP-4	2

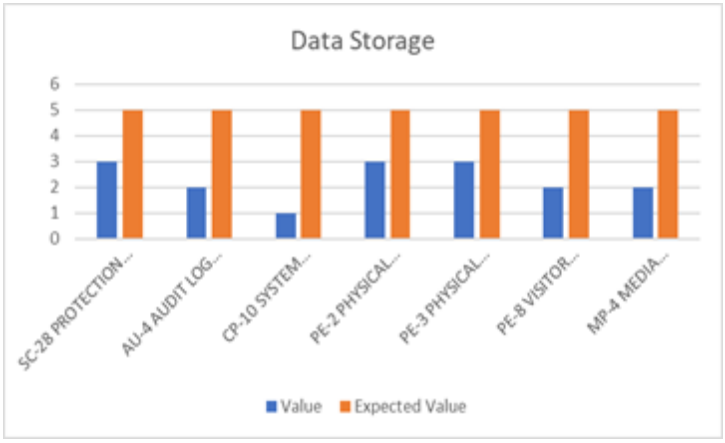

Figure 3. *Maturity Level of Data Storage*

Table 8 and figure 3, show the results of measuring the maturity level for the objective of data storage. The organization has implemented control clauses SC-28, PE-2, and PE-3 in a documented manner (level 3 – defined). This shows the organization has a system to protect information when it is stored, has a physical restriction mechanism, and implements verification for individuals who enter one of the data storage facilities. Furthermore, there is one of the lowest measurement values (level 1 – initial) in the controlling clause of CP-10. The organization does not yet have a well-documented mechanism for system recovery and reconstitution in the event of system disruptions, leaks, and failures. Organizations do so reactively, and inconsistently. In addition to the controlling clause, the organization has started to carry out control with a repetitive pattern even though it has not been appropriately documented and implemented (level 2 – repeatable).

Table 9. Maturity Level of Data Backup

Objective	NIST SP800-53 Rev 5 Control	Value
(DBU) Data backup	SC-28	3
	CP-6	3
	CP-9	2

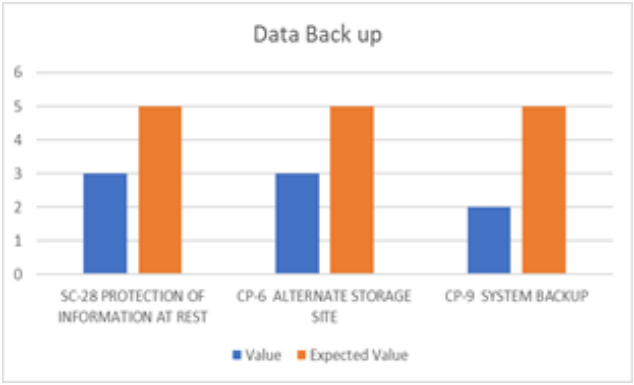

Figure 4. *Maturity Level of Data Backup*

One of the most critical things in handling potential digital evidence is a data backup mechanism. The results of the maturity level measurements can be seen in table 9 and figure 4. Of the 3 control clauses, there are 2 control clauses SC-28 and CP-6 which are already at level 3 – defined. While 1 control clause CP-9 at level 2 – repeatable. This shows that the organization already has a system for the security of information at rest, has alternative storage places, and the necessary agreements to store backup information. This helps organizations maintain the confidentiality, integrity, and availability of data. However, the organization still does not have a well-documented user information backup system despite having a repetitive habit of control. This will pose an availability threat to the organization in the possibility of user system problems.

Table 10. Maturity Level of Documentation

Objective	NIST SP800-53 Rev 5 Control	Value
(DOC) Documentation	SA-5	2
	CM-3	2

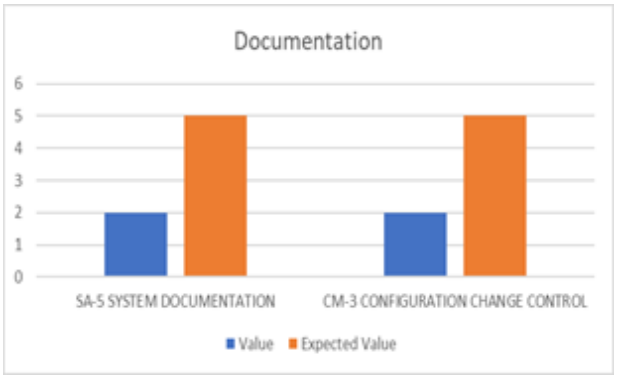

Figure 5. *Maturity Level of Documentation*

In handling potential digital evidence, the documentation process is crucial. The results of the maturity level measurements can be seen in table 10 and figure 5. The control clauses SA-5 and CM-3 have a maturity value of 2 – repeatable. Organizations already

have a recurring pattern but do not yet have documented controls for the administrator's documentation process for systems, components, and services as well as in reporting changes to their configuration-controlled systems, reviewing system and data changes, analyzing security and privacy impacts, and keeping records of changes from time to time. This will be able to disrupt data integrity.

Table 11. Maturity Level of Identification and Classification

Objective	**NIST SP800-53 Rev 5 Control**	**Value**
(DIC) Data Identification and Classification	MP-7	2
	SI-10	2
	MP-3	1

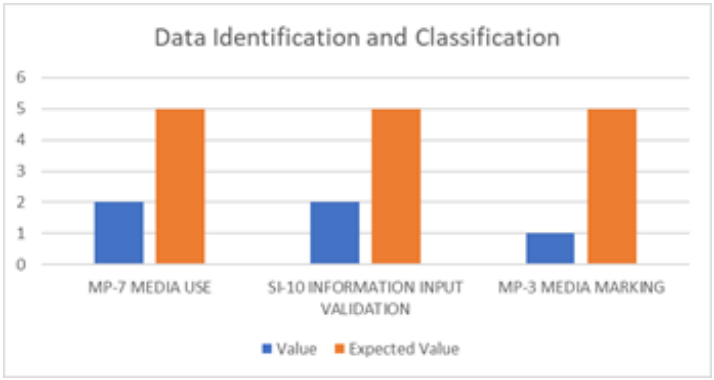

Figure 6. *Maturity Level of Data Identification and Classification*

Table 11 and figure 6 show the results of measuring the maturity level on the identification and classification of data. Control clauses MP-7 and SI-10 have a maturity value of level 2 – repeatable. Organizations already have a recurring pattern but do not yet have a documented mechanism to limit the use of portable media, such as restrictions on access to input, read, and write on storage media as well as a means to validate the information entered into the system. This may cause a privacy invasion of the information available. There is one of the lowest measurement values (level 1 – initial) in the MP-3 control clause. This shows that the organization does not yet have a mechanism to mark media to provide a sign of distribution restrictions and control mechanisms for unclassified information, which results in user errors in processing information.

Table 12. Maturity Level of Collection and Acquisition

Objective	**NIST SP800-53 Rev 5 Control**	**Value**
(CLA) Collection and Acquisition	MP-4	2
	MP-5	2
	MP-7	2

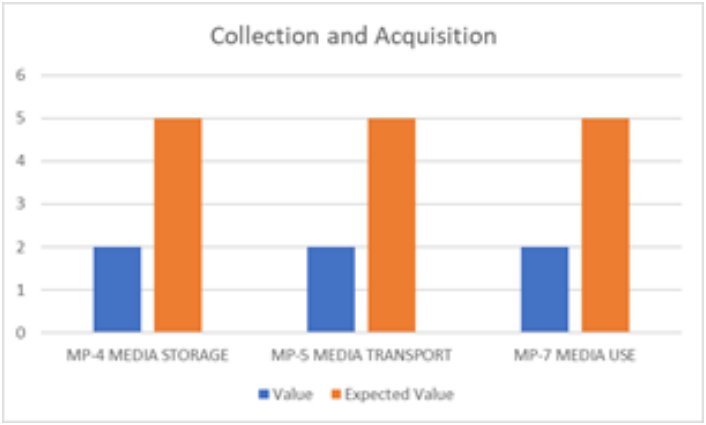

Figure 7. Maturity Level of Data Collection and Acquisition

The results of the maturity level measurements can be seen in table 12 and figure 7. The control clauses for MP-4, MP-5, and MP-7 have a maturity value of level 2 – repeatable. The organization already has a recurring pattern but does not yet have a documented control in conducting an inventory, ensuring inspection procedures, and maintaining accountability for stored physical media (HDD, SSD, Flash Disk, etc). Likewise, the management of removable data, and technical and non-technical controls on restrictions on media use. This can lead to security breaches of confidentiality and integrity.

Table 13. Maturity Level of Data Return

Objective	**NIST SP800-53 Rev 5 Control**	**Value**
(DRT) Data return	MP-8	1

Figure 8. *Maturity Level of Data Return*

One of the critical processes in handling potential digital evidence is the return of data that is no longer relevant to the case based on legal reviews by investigators, prosecutors, or judges. The results of the maturity level measurements can be seen in table 13 and figure 8. The MP-8 control clause has a value of 1 – initial. This shows that the organization does not yet have security rules, and is still acting reactively without previous careful planning.

Table 14. Maturity Level of Data Eradication

Objective	**NIST SP800-53 Rev 5 Control**	**Value**
(DER) Data eradication	MP-6	3

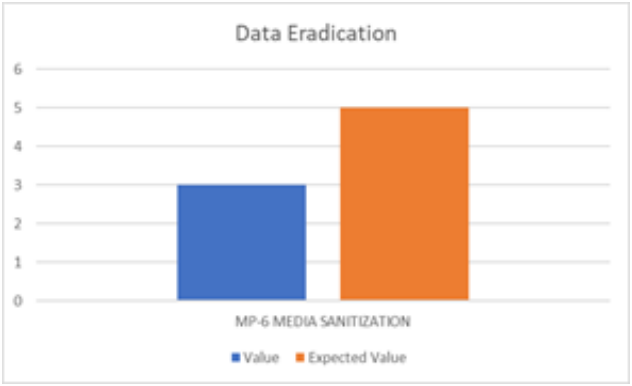

Figure 9. *Maturity Level of Data Eradication*

Finally, there is a clause on the objective of eradicating data. The results of the maturity level measurement can be seen in table 14 and figure 9. The organization has a value of 3 – defined on the MP-6 control clause, indicating that the organization has documented controls for the mechanism for deleting digital evidence data, operational documents, and systems that are no longer available used. This is a good step for the organization, although the institution still needs to improve it to reach level 5 – optimizing.

4.3 Overall Maturity Level

The results of measuring the maturity level of 30 security controls show that most of the controls have not been fully implemented by the organization, with 17 controls still at level 2 (repeatable), which means the organization already has a repeating pattern related to potential digital evidence information management activities but has not well defined, which will leave the organization vulnerable to security and privacy issues. The organization also has 4 controls that are at level 1 (initial), meaning that the organization still applies these controls reactively without being preceded by planning, so that there are inconsistencies and poses a heightened security risk. Furthermore, the organization has 9 controls at level 3 (defined) which means that it already has security and privacy controls that are socialized to all employees, well documented. More details can be seen in table 15.

Table 15. Quantity of Maturity Level

Maturity	**Quantity**
0 - Non-Existing	0
1 – Initial	4
2 - Repeatable	17
3 – Defined	9
4 - Quantitively Managed	0
5 - Optimizing	0

Table 16. Overall Maturity Level

Objective	**Maturity**	**Rating**
DTR	2,2	Repeatable
DST	2,29	Repeatable
DBU	2,67	Repeatable
DOC	2	Repeatable
DIC	1,67	Initial
CLA	2	Repeatable
DRT	1	Initial
DER	3	Defined
Overall Maturity:	**2,10**	**Repeatable**

After getting the overall score, it can be seen in table 16 that the organizational maturity level in handling potential digital evidence in the integrated criminal justice system is at the repeatable level with a value of 2.1.

4.4 Gap Analysis

Based on the results of the calculation of the information security maturity level, the organizational maturity level is currently at 2.1 (repeatable) to get the best maturity level 5 - optimizing, there is still a gap of 2.9.

Table 17. Gap Analysis

Objective	**Maturity**	**Expected**	**Gap**
DTR	2,2	5	2,8
DST	2,29	5	2,71
DBU	2,67	5	2,33
DOC	2	5	3
DIC	1,67	5	3,33
CLA	2	5	3
DRT	1	5	4
DER	3	5	2
Overall:	2,1	5	2,9

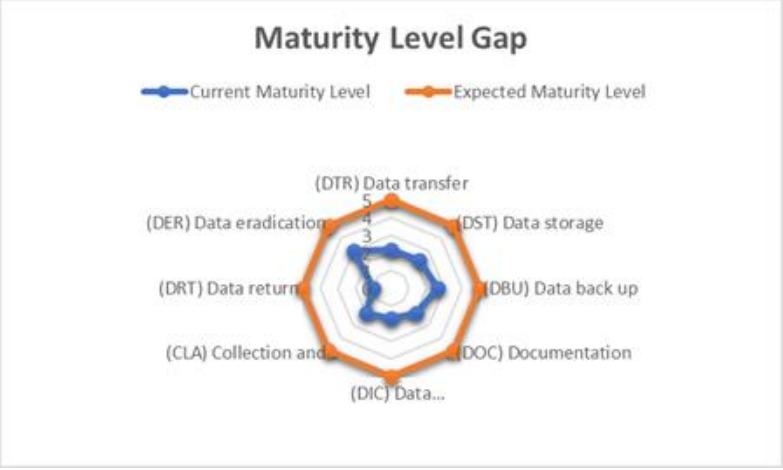

Figure 10. *Maturity Level Gap*

V. Conclusion

The results of the organizational maturity level using NIST Maturity in the process of handling potential digital evidence in the criminal justice system in the XYZ organization, the current state is 2.1, meaning that it is at level 2 (repeatable) from the range 0-5. In the process, there are 8 objective clauses and 30 information security and privacy control clauses of NIST SP 800-53 Rev 5 which are measured using NIST Maturity. The outcomes represent the condition of the organization which in general already has a repeating pattern but has not been well documented and socialized to employees. The result of calculating the gap value with the expected conditions is 2.9. The gap obtained is quite large, so organizations need to implement each control optimally, integrate it, and refer to "best practice". According to the controlling clause, the maturity of 4 controls is worth 1 (initial), the maturity of 17 controls is worth 2 (repeatable), the maturity of 9 controls is worth 3 (defined), and no control maturity is worth 0 (non-existing), 4 (quantitively managed), and 5 (optimizing). These results are part of the organization's planning evaluation process to improve security controls.

References

Anderson, Philip., and European Union. European Network and Information Security Agency. 2014. *Electronic Evidence, a Basic Guide for First Responders : Good Practice Material for CERT First Responders.*, ENISA.

Arshad, H., Jantan, A. bin, and Abiodun, O. I. 2018. "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *Journal of Information Processing Systems* (14:2), Korea Information Processing Society, pp. 346–376. (https://doi.org/10.3745/JIPS.03.0095).

Avianto, H., and Ogi, D. 2019. "Design of Electronic Medical Record Security Policy in Hospital Management Information System (SIMRS) in XYZ Hospital," in *2019 2nd International Conference on Applied Information Technology and Innovation (ICAITI)*, KCG College of Technology, pp. 163–167. (https://doi.org/10.1109/ICAITI48442.2019.8982122).

Cipher, "NIST Maturity Self-Assessment Survey," https://info.cipher.com/nist-maturity-self-assessment-survey accessed 10/02/2022.

"Constitution of Indonesia 8/1981 about Criminal Procedure Law." 1981. Jakarta.

"Constitution of Indonesia 11/2008 about Information and Electronic Transactions." 2008. Jakarta.

"Constitution of Indonesia 20/2001 about Eradication of Corruption." 2001. Jakarta.

Dananjaya, N. S. 2014. "Sistem Peradilan Pidana Terpadu (Integreted Criminal Justice System) Di Kaji Dari Perspektif Sub Sistem Kepolisian". Vyavahara Duta, 9 (1). ISSN 1978-0982 (https://erepo.unud.ac.id/id/eprint/11614)

Feri Efendi, T., Rahmadi, R., and Prayudi, Y. 2020. "Rancang Bangun Sistem Untuk Manajemen Barang Bukti Fisik Dan Chain of Custody (CoC) Pada Penyimpananan Laboratorium Forensika Digital," *Jurnal Teknologi Dan Manajemen Informatika* (6:2), pp. 53–63. (https://doi.org/10.26905/jtmi.v6i2.4177).

"ISO/IEC 27037:2012 Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence." 2012.

Kohar, A., Riadi, I., and Lutfi, A. 2015. "Analysis of Smartphone Users Awareness Activities Cybercrime," *International Journal of Computer Applications* (129:2), Foundation of Computer Science, pp. 1–6. (https://doi.org/10.5120/ijca2015906449).

Kurniawan, E., and Riadi, I. 2018. "Security Level Analysis of Academic Information Systems Based on Standard ISO 27002:2003 Using SSE-CMM," *International Journal of Computer Science and Information Security* (16), pp. 139–147. (https://doi.org/10.13140/RG.2.2.20925.15840).

Le, N. T., and Hoang, D. B. 2016. "Can Maturity Models Support Cyber Security?," in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, Las Vegas, NV, USA: IEEE, December 9. (https://doi.org/10.1109/PCCC.2016.7820663).

Mukasey, M. B., Sedgwick, J. L., and Hagy, D. W. 2001. "Special REPORT Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition," Washington DC. (www.ojp.usdoj.gov/nij).

NIST SP800-53 Revision 5 - Security and Privacy Controls for Information Systems and Organizations." 2020. Gaithersburg, MD, September 23. (https://doi.org/10.6028/NIST.SP.800-53r5).

Niati, D. R., Siregar, Z. M. E., & Prayoga, Y. (2021). The Effect of Training on Work Performance and Career Development: The Role of Motivation as Intervening Variable. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, *4*(2), 2385–2393. https://doi.org/10.33258/birci.v4i2.1940

Nugroho, S. A. 2010. "Analisis Kedudukan Dan Kekuatan Pembuktian Digital Evidence Dalam Pembuktian Perkara Korupsi (Suatu Studi Terhadap UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan UU Nomor 20 Tahun 2001 Tentang Pemberantasan Tindak Pidana Korupsi)," Semarang.

Prayudi, Y. 2014. "Problema Dan Solusi Digital Chain of Custody Dalam Proses Investigasi Cybercrime," *Seminar Nasional Aplikasi Teknologi Informasi (Senasti)*, pp. 197–204.

R, R., Riadi, I., and Prayudi, Y. 2016. "A Maturity Level Framework for Measurement of Information Security Performance," *International Journal of Computer Applications* (141:8), Foundation of Computer Science, pp. 1–6. (https://doi.org/10.5120/ijca2016907930).

Supriyatna. 2009. "KUHAP DAN SISTEM PERADILAN PIDANA TERPADU," in *Wacana Hukum, 8(1)* (Vol. VIII), Surakarta, September 27. (https://doi.org/10.33061/1.jwh.2009.8.1.318).

Tian, Z., Li, M., Qiu, M., Sun, Y., and Su, S. 2019. "Block-DEF: A Secure Digital Evidence Framework Using Blockchain," *Information Sciences* (491), Elsevier Inc., pp. 151–165. (https://doi.org/10.1016/j.ins.2019.04.011).

Yoga Pradana, F., and Trianto, N. 2018. "Privacy Control for Personally Identifiable Information on the Information System (Case Study:XYZ Organization)," in *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*, KCG College of Technology, pp. 50–55. (https://doi.org/10.1109/ICAITI.2018.8686766).