

# RISK ANALYSIS OF HUMAN RESOURCE INFORMATION SYSTEMS USING COBIT 5

<sup>1</sup>EVARISTUS DIDIK MADYATMADJA, <sup>2</sup>LYDIA LILIANA,  
<sup>3</sup>JOHANES FERNANDES ANDRY, <sup>4</sup>HENDY TANNADY

<sup>1</sup>Information Systems Department, School of Information Systems, Bina Nusantara University, Indonesia

<sup>2,3</sup> Information Systems, Universitas Bunda Mulia, Faculty of Technology and Design, Indonesia

<sup>4</sup> Department of Management Universitas Pembangunan Jaya Banten, Indonesia

E-mail: <sup>1</sup>emadyatmadja@binus.edu, <sup>2</sup>lydialiliana6@gmail.com, <sup>3</sup>jandry@bundamulia.ac.id,  
<sup>4</sup>hendy.tannady@upj.ac.id

## ABSTRACT

Information technology is an important key in the company because it offers efficiency and authority to achieve goals. This can be seen from the development of technology in pharmaceutical companies in Jakarta that use Human Resource Information Systems (HRIS). HRIS provides services in the form of management information for all employees in the company. Currently, not many have conducted risk analysis on the information systems used. On the one hand, information systems have become a part that is difficult to access in almost every business process in the company. The use of technology can present threats that can affect applicable risks. Therefore, companies need to pay attention to risk management to anticipate the dangers that can occur. The study uses the COBIT 5 framework to analyze the risks that occur in the company by using the domain Monitor, Evaluate, Assessment MEA02 because it is related to the transparency process for the main stakeholders regarding the appropriateness of the internal control system so that it can ensure the achievement of company goals and objectives and provide sufficient knowledge about the system risk of human resource information. The research starts from references, determines the domains and processes used, analyzes HRIS, compiles interview lists, analyzes interview results, calculates process capability models from HRIS implementation and analyzes HRIS to risk management. The output of this study is the acquisition of risk management documents in pharmaceutical companies that contain lists of risks, level risks, impacts, risks, and the results of recommendations using the MEA02 domain from COBIT 5 and a SWOT analysis.

**Keywords:** *COBIT 5, Monitor-Evaluate-Assess (MEA), Human Resource Information System (HRIS).*

## 1. INTRODUCTION

Information Technology is one of the ways used to support information system processing [1]. IT works in every system, the aim is to help and support management in solving structured problems [2]. Information technology (IT) has become an important part of organizations and organizations. The services provided by IT provide the ability for them to meet the needs of their citizens or customers [3]. Information technology (IT) is an important part of organizations and companies [4], one of them is in a pharmaceutical company located in Jakarta. This pharmaceutical company focuses on producing drugs. Companies are supported by the role of technology to help maintain the implementation of their business processes in Indonesia in order to achieve effectiveness and efficiency [5].

Information technology has added value to influence companies in implementing business processes [6]. This can be seen from the ability of information technology to support changes in business processes that occur in the company [7]. Data is compiled and managed in information systems, one of which is the application of Human Resources Information Systems (HRIS). Every large company certainly has a qualified HRIS. HRIS is a computerized system for obtaining, storing, manipulating and analyzing capabilities to be used to help the process of distributing information about an organization's human resources [8]. This system helps businesses in developing the composition of staffing needs, identifying prospective new employees; keeping employee records, tracking employee training, skills, and performance, and helping managers develop plans that are compatible

with employee compensation and career development [9].

HRIS provides services in the form of management information for all employees, report information and analysis of employees, administrative registration, status changes, and updating personal information, complete integration with company management software [10]. Without the role of the human resource information system, companies will find it difficult to manage human resources [11]. One company that has a human resource information system is a company engaged in the field of pharmaceuticals or medicines.

HRIS is used by pharmaceutical companies to help monitor the performance of the company's employees so that management can find out the performance of its employees. This research will focus on risk management by balancing business strategy and risk management, so that it is expected to help companies get optimal results from business process activities. The author uses the COBIT 5 framework to identify risks from human resource information systems with the process used is MEA02. The MEA domain itself consists of 3 processes namely MEA01, MEA02 and MEA03.

The application of the MEA02 domain in HRIS is due to the fact that over time the use of HRIS is increasing to help company business processes. This causes the higher risk of implementing HRIS which needs to pay attention to the risk of digital threats and physical threats at the time of its implementation. The use of the MEA02 domain is considered to be able to measure HRIS readiness to face all possibilities that result in failure of information technology services. By carrying out a risk analysis on HRIS using the MEA02 domain, it can be done to control the risks in the planning process, regulate and maintain risk management standards when implementing HRIS.

The author chooses to use the MEA02 (Monitor, Evaluate and Assess the System of Internal Control) process because it is related to helping get transparency to key stakeholders about the feasibility of an internal control system so as to guarantee operations, guarantee the achievement of company goals and objectives and provide sufficient knowledge about human resource information system risk [12]. Based on the selection of the MEA02 domain to be applied to HRIS, the research hypothesis is that "It is suspected that pharmaceutical companies in implementing risk analysis are at a stage where the risk management process has been managed, planned properly and has

been defined into a Standard Operating Procedure (SOP), guidance and other written rules". Therefore, the output of this research is the acquisition of risk management documents in pharmaceutical companies which lists risk, risk level, impact, risk management and the results of recommendations using the MEA02 domain from COBIT 5 and SWOT analysis.

2. LITERATURE REVIEW

2.1 Previous Research

The authors will discuss previous research about COBIT and Human Resources Information Systems, Based on an International Journal of Open Information Technologies entitled "Assessment IT Governance of Human Resources Information System Using COBIT 5" written by, J. F. Andry, Hartono and Aziza Chakir [23], the following conclusions can be drawn are as follows:

- a) The equation with this report is related to the risk assessment and measurement that uses the principles of COBIT 5.
- b) The difference with this report is gap analysis and recommendations sub domain DSS02.
- c) The strength of this journal is that it focuses on SWOT analysis and recommendations sub domain MEA02.
- d) The weakness of this journal is that it does not have an explanation of security technical about HRIS.

2.2 COBIT 5

COBIT 5 is one of the business frameworks for improving corporate governance and management [13]. COBIT 5 helps companies get the most value from IT utilization by maintaining a balance between being aware of the benefits and optimizing the level of risk and the use of resources [14].

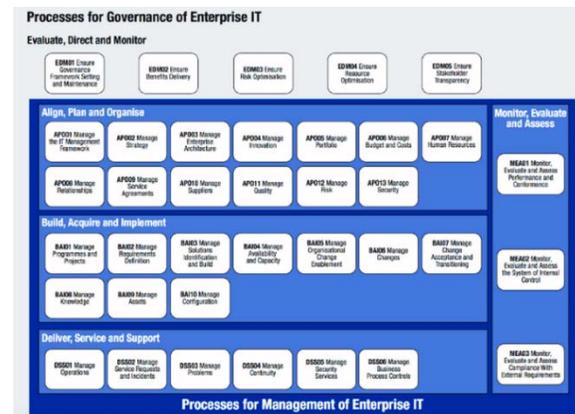


Figure 1: Processes For Governance of Enterprise IT [15]

Based on Figure 1 Processes for Governance of Enterprise IT, the current version of the framework, COBIT 5, was released in 2012. The COBIT 5 process reference model is the successor to the COBIT 4.1 process model. The COBIT 5 Process Reference Model shows a complete set of 37 governance and management processes in COBIT 5. The current version of the framework, COBIT 5, was released in 2012. The COBIT 5 process reference model is the successor to the COBIT 4.1 process model. The COBIT 5 Process Reference Model shows a complete set of 37 governance and management processes in COBIT 5.

**2.3 Monitor, Evaluate, Assess (MEA)**

The focus of the MEA domain on COBIT 5 is on the management area for the process of assessing the needs of the company and the current system that is still fulfilling or not, ensuring the design and control complies with regulations, and monitoring relating to independent assessment, effectiveness and ability to meet business objectives by independent evaluators [16].

*Table 1: COBIT 5 Process Capability Model [17]*

Index	Description
Index 0: Incomplete Stage	Implementation of the process was not carried out so that the process objectives were not met. At this stage, there is little evidence of achievement and not carried out systematically.
Index 1: Performed Stage	Measurements were made on the application of the process whether it met its objectives so that each process obtained output that was in line with expectations.
Index 2: Managed Stage	Conduct planning, monitoring and evaluating the results of the implementation of the process and determine, control and maintain the results of the work products of the process.
Index 3: Established Stage	The process has been defined and gets the desired process output.
Index 4: Predictable Stage	There is already a definition of boundaries that is used to get the results of the process so that the process can be run following the specified limits.
Level 5: Optimizing Stage	Make continuous improvements so that the company's goals can be achieved in the present and future.

Based on Table 1 COBIT 5 Process Capability Model, it is a process capability assessment model to identify the level of certain process capability and then determine the next steps to improve the process capability.

The MEA02 Domain Monitor, Evaluate and Assess the System of Internal Control, monitors and

evaluates the control environment including self-assessment and independent assurance reviews. Allows management to identify control deficiencies and in-efficiency to initiate corrective actions. Plan, regulate and maintain standards for internal control and assurance assessment activities. Consists of 8 subdomains, namely: MEA02.01 Monitor Internal Controls, MEA02.02 Review Business Process Controls Effectiveness, MEA02.03 Perform Control Self-assessments, MEA02.04 Identify and Report Control Deficiencies, MEA02.05 Ensure That Assurance Providers are Independent and Qualified, MEA02.06 Plan Assurance Initiatives, MEA02.07 Scope Assurance Initiatives and MEA02.08 Execute Assurance Initiatives [16].

*Table 2: COBIT 5 Process Capability Model [19]*

Scale	Description	Achievement
N	Not performed	0 – 14.99%
P	Partially performed	15.00 – 49.99%
L	Largely performed	50.00 – 84.99%
F	Fully performed	85.00 – 100%

In addition, each attribute is classified using a standard rating scale described in the ISO/IEC 15504 standard. These ratings consist of [18] (shown in Table 2 COBIT 5 Process Capability Model). Based on Table 2 COBIT 5 Process Capability Model, it is the standard rating scale described in the ISO/IEC 15504 standard. N scale is not achieved where there is little or no evidence of achievement of the completeness specified in the assessed process. The P scale is achieved partially with some evidence and achievement of the completeness specified in the assessed process. Some aspects of achieving completeness may not be predictable. The L scale is for the most part with no evidence of a systematic approach, and significant achievement of the completeness specified in the process being assessed. Some weaknesses related to this completeness may exist in the process being assessed. The F scale is fully achieved, achievement with no evidence of a complete systematic approach, and full achievement of the completeness specified in the process being assessed. There were no significant weaknesses related to this completeness in the assessed process.

**2.4 SWOT Analysis**

SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) SWOT analysis is the systematic identification of various factors to formulate a company's strategy [20]. The SWOT analysis aims as a consideration in providing recommendations in order to avoid recommendations that go beyond the capabilities of

the agency [21]. This analysis is based on logic that can maximize strengths and opportunities, but simultaneously minimize weaknesses (Weaknesses) and threats (Threats). SWOT analysis is also carried out by describing the strengths of opportunities, strengths of threats, weaknesses of opportunities and weaknesses of threats. The strategy decision making process is always related to the development of the company's mission, goals, strategies and policies. Thus, strategic planning must analyze the company's strategy factors (strengths, weaknesses, opportunities and threats) in the current conditions [22].

**3. RESEARCH METHODOLOGY**

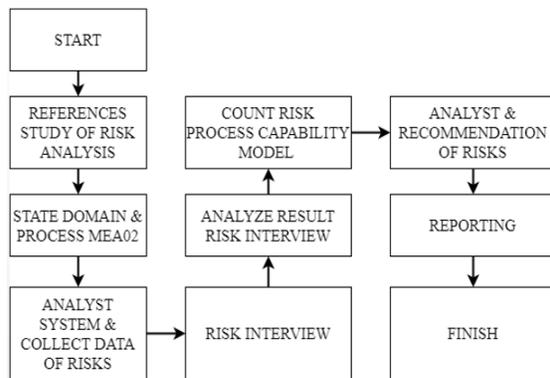


Figure 2: Index Level Steps Process Capability Model [23]

Based on Figure 2 Index Level Steps Process Capability Model, it is known that this research starts from:

1. References Study of Risk Analysis. Study previous research and books relating to risk analysis, risk management and risk level.
2. State Domain and Process. Define the domains used in this study, namely MEA02 Monitor, Evaluate, and Assess the System of Internal Control and the process of collecting data directly to the company.
3. Analyst System and Collect Data Of Risks. Analyze the HRIS and collect data about the risks of implementing HRIS.
4. Risk Interview. Compile a list of interview questions about the MEA02 process and direct interviews to the research location.
5. Analyst Result Risk Interview. Analyzing the answers to interview questions that have been asked of the interviewees.
6. To count Risk Process Capability Model. Calculate the process capability model to determine the capability level of the risks that exist in the Human Resource Information System (HRIS) system.
7. Analyst and Recommendation Of Risks. Conduct an analysis of the risk register, risk level, impact, and risk management of the HRIS.
8. Reporting. Make a report of all the risks that exist in the HRIS and provide recommendations based on the MEA02 domain.

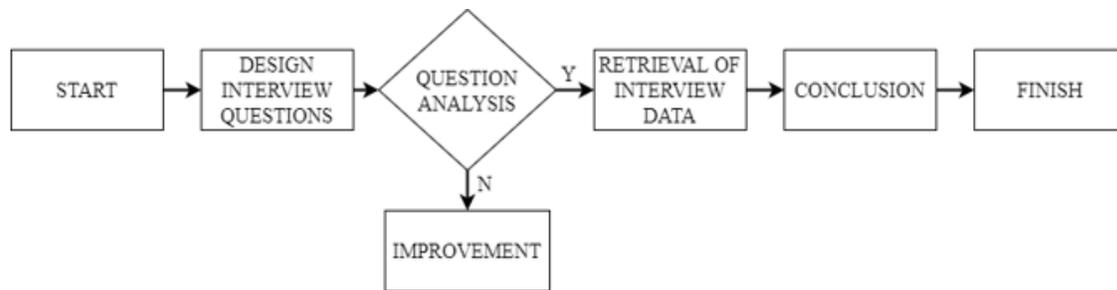


Figure 3: Interview Stage [23]

Based on Figure 3 Interview Stage, it is known that the interview stage starts from the design of interview questions relating to MEA02, do a question analysis. However, if the analysis is not suitable, the interview questions will be improved. After that, conclusions can be drawn from the results of interviews conducted with the speakers

**4. RESULT AND ANALYSIS**

**4.1 Finding Results of MEA02**

In this section, the authors describe the results of the MEA02 findings, the results of the MEA02 sub-process recommendations and the results of the SWOT analysis.

**4.1.1 MEA02.01 Monitor Internal Controls**

MEA02.01 is monitoring on an ongoing basis, setting standards and developing IT environment controls and control frameworks to achieve organizational goals. The findings obtained from the MEA02.01 sub-process are:

1. The availability of SOPs from the fingerprint attendance.
2. Fingerprint attendance users have followed the applicable SOP, if violated they will be hit by a warning.
3. IT internal control over attendance programs for risk assessment is currently running according to organizational goals.
4. Internal IT control of attendance programs for risk assessment is carried out effectively and efficiently.

#### 4.1.2 MEA02.02 Review Business Process Controls Effectiveness

MEA02.02 is to provide a review for the operation of controls, including reviews for monitoring and test evidence, to ensure the existing controls in the business operate effectively. The findings obtained from the MEA02.02 sub-process are:

1. The company already understands and prioritizes system risk towards the organization's goals.
2. Never happened hardware and fingerprint time attendance network damage, because the company's head office offline.
3. Possible risks arising from the application of this fingerprint attendance.

#### 4.1.3 MEA02.03 Perform Control Self-assessments

MEA02.03 is encouraging management and owners to take positive ownership of development control through internal assessment programs. The findings obtained from the MEA02.03 sub-process are:

1. There has been a development of the ongoing risk self-assessment program for the current attendance program.
2. Any such risk if it occurs in the company has a low frequency, because the mistakes are not often even almost non-existent, because the IT department has maintained the entire IT system in this company.
3. Obtaining a self-assessment has been compared with current industry standards.

#### 4.1.4 MEA02.04 Identify and Report Control Deficiencies

MEA02.04 is to identify control deficiencies, analysis, identify the root of these deficiencies. The findings obtained from the MEA02.04 sub-process are:

1. There are limits to the risk control of using fingerprint attendance.
2. The causes of each of these risks have been previously described.

#### 4.1.5 MEA02.05 Ensure That Assurance Providers are Independent and Qualified

MEA02.05 is this assurance that assurance providers are independent and qualified is to ensure the rights of the guarantee agent are independent of the functions, groups, or scope of the organization. The findings obtained from the MEA02.05 sub-process are:

1. There is already a guaranteed standard for the use of fingerprint technology in terms of risk control.
2. Fingerprint attendance hardware providers have provided effective and efficient services to support the use of attendance hardware.

#### 4.1.6 MEA02.06 Plan Assurance Initiatives

MEA02.06 are planning a guarantee initiative based on company objectives and priority strategies, inherent risks, resource constraints and insufficient knowledge about the company. The findings obtained from the MEA02.06 sub-process are:

1. The Company has controlled risk from internal threats arising from the use of fingerprint attendance.
2. The Company has carried out risk control from external threats arising from the use of fingerprint attendance.
3. To overcome internal risks, periodically check the hardware by the IT department, fearing dust / rust. In terms of network, fear that the infrastructure is damaged because the cable is broken. So the IT team is responsive in checking it before it is used, because this fingerprint attendance makes it easier for us to check whether employees are entering or not. When viewed from the external side, of course, from the human resources has given SOP from the fingerprint attendance like this, so as to minimize errors.

#### 4.1.7 MEA02.07 Scope Assurance Initiatives

MEA02.07 this scope of assurance initiatives is to define and agree with the management of the scope of initiative guarantees based on objective guarantees. The findings obtained from the MEA02.07 sub-process are:

1. The scope of attendance risk handling has been determined to identify the company's objectives.
2. The emergence of the consequences of risks can be predicted.
3. The practice of collecting and evaluating absentee risk information has been carried out.

#### 4.1.8 MEA02.08 Execute Assurance Initiatives

MEA02.08 Execute assurance initiatives are implementing a guarantee initiative plan, making reports on identified findings, providing positive assessment opinions, where needed, and recommending to develop identified operational performance. The findings obtained from the MEA02.08 sub-process are:

1. Identification and application of corrective actions arising from the assessment and reporting of internal IT controls on the risks of applying attendance have been carried out.
2. Corrective action has been taken by IT control of attendance program risks.

Following are the findings of each sub-process, the following is described the identification of causes, causes of risk, risk impacts from the implementation of the Human Resource Information System (HRIS) from the internal and external sides.

Table 3: Analysis of the Causes and Impacts Of Risks External

No	Risk	Frequency Occurs	Cause Of Risk	Impact Risk
1	Data theft and data modification by irresponsible parties.	Low	System and firewall security for data access is not strong enough.	Company data is duplicated and used by irresponsible parties.
2	Human resource error in the use of HRIS.	Low	Lack of training / training in the use of HRIS.	The use of HRIS is hampered.

Based on Table 3 Analysis of The Causes and Impacts Of Risks External, the results of risk analysis in terms of risk, level of risk, risk, and risk for the company. It is estimated that there are 2 external risk factors that affect the performance of the Human Resources Information System (HRIS), namely theft of data from HRIS and modification by certain parties in order to bring profit. This risk is

included in the low frequency because it never happened in the company. This risk arises because the security of HRIS and the firewall is still lacking. If this risk is ignored, duplicate data will be needed.

The second risk that arises is the source of human error or can be caused by human error. This is caused by the lack of training or training in using HRIS.

Table 4: Analysis of the Causes and Impacts of Risks Internal

No	Risk	Frequency Occurs	Cause Of Risk	Impact Risk
1	Damage to hardware	Low	Hardware exposed to dust, overheat, rust, natural disasters, fire.	The hardware cannot be operated.
				Inhibiting the process of data collection on human resources.
2	Damage to the HRIS network	Low	Network infrastructure is damaged due to broken cables, slow internet.	HRIS cannot be used.
				Inhibiting the withdrawal of HRIS data.
3	Server performance is unstable and starts to decline.	Low	Server traffic increased due to many accesses.	HRIS cannot pull attendance data / error occurs.
4	Server memory malfunctions.	Low	Server storage capacity has been used a lot	Reducing server operating performance.
5	The server is too hot.	Low	HRIS server temperature is hotter than room temperature.	The internet network has temporarily been paralyzed,
6	HRIS network cable is not connected (damaged).	Low	Incorrect cable setup.	Internet access and data transmission have failed.
7	Unable to send or receive data and information from users / servers.	Low	Interrupt.	Data access failure.
8	Damage to HRIS system for employee / HRD PCs.	Low	Error installing or configuring the HRIS system.	Interrupt software.
9	Damage to network infrastructure.	Low	System security for network access is not good.	Data transmission failure.
			Error installing or configuring the HRIS system.	
10	The HRIS system does not detect human resource data in the company.	Low	An interruption occurs when retrieving HRIS system data.	Data cannot be accessed quickly when needed.

Based on Table 4 Analysis of The Causes and Impacts of Risks Internal, it is explained that there are 10 types of risks that may arise in the implementation of Human Resource Information System of pharmaceutical companies. The 10 types of risks such as damage to hardware, damage to the HRIS network, server performance is unstable and begins to decline, server memory malfunctions, the server is too hot, HRIS network cable is not connected (damaged), unable to send or receive data and information from users / server, damage to the HRIS system for employee PCs / HRD, damage to the network infrastructure and HRIS system does not detect human resource data in the company. Each risk is classified as a low level and an analysis of the causes of risk emergence up to the impact caused by each risk.

After analyzing the risks that arise from the Human Resource Information System (HRIS), the process attribute mapping is determined. After that the average capability of each sub-process in the MEA02 domain is calculated.

Based on Table 5 MEA02 Mapping Process Attributes, the MEA02.01 sub-process has reached capability level 3 because it has fully achieved PA 1.1 through PA 3.2. The MEA02.02 sub-process has reached capability level 3 because it has fully achieved PA 1.1 through PA 3.2. The MEA02.03 sub-process has reached capability level 3 because it has fully achieved PA 1.1 through PA 4.1. MEA02.04 has reached capability level 3 because it has fully achieved PA 1.1 through PA 4.1. MEA02.05 has reached capability level 3 because it has fully achieved PA 1.1 through PA 3.2. The MEA02.06 sub-process has reached capability level 3 because it has fully achieved PA 1.1 through PA 3.2. The MEA02.07 sub-process has reached capability level 3 because it has fully achieved PA 1.1 through PA 3.2. The MEA02.08 sub-process has reached capability level 3 because it has fully achieved PA 1.1 through PA 3.2.

After mapping the process attributes as table 5, an average capability level for each MEA02 sub-process domain is calculated.

Table 5: MEA02 Mapping Process Attributes

Sub-proses	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
MEA02.01	F	F	F	F	F	N	N	N	N
MEA02.02	F	F	F	F	F	N	N	N	N
MEA02.03	F	F	F	F	F	F	N	N	N
MEA02.04	F	F	F	F	F	F	N	N	N
MEA02.05	F	F	F	F	F	N	N	N	N
MEA02.06	F	F	F	F	F	N	N	N	N
MEA02.07	F	F	F	F	F	N	N	N	N
MEA02.08	F	F	F	F	F	N	N	N	N

Table 6: Capability Level MEA02

MEA02 Monitor, Evaluate and Assess The System of Internal Control			
Sub-processess	Description	Process Attributes	Results
MEA02.01	Monitor Internal Controls	3.2	3
MEA02.02	Review business process controls effectiveness	3.2	3
MEA02.03	Perform control self-assessments	4.1	3
MEA02.04	Identify and report control deficiencies	4.1	3
MEA02.05	Ensure that assurance providers are independent and qualified	3.2	3
MEA02.06	Plan assurance initiatives	3.2	3
MEA02.07	Scope assurance initiatives	3.2	3
MEA02.08	Execute assurance initiatives	3.2	3
Average			3

Based on Table 6 Capability Level MEA02, the MEA02 Monitor, Evaluate and Assess the System of Internal Control process shows that the average capability level is 3. In MEA02.01, reaches PA 3.2 and has a capability level 3. For MEA02.02, it reaches PA 3.2 and has capability level 3. MEA02.03, reaches PA 4.1 and has capability level 3. MEA02.04 reaches 4.1 and has capability level 3. MEA02.05 reaches PA 3.2 and has capability level 3. MEA02.06 reaches PA 3.2 and has capability

level 3. MEA02.07, reaches PA 3.2 and has a capability level 3. MEA02.08, reaches PA 3.2 and has a capability level 3.

MEA02.01 fully achieved PA 3.2 because the internal IT risk control standard against HRIS has been running effectively and efficiently. MEA02.02 fully achieved PA 3.2 because HRIS standards are managed by internal IT control processes and have been implemented well. MEA02.03 fully achieved PA 4.1 because self-assessment of HRIS risk has

been measured, the extent to which the measurement results are used to ensure the implementation of the process can support the achievement of organizational goals, but the measurement results have not reached the limits that have been previously defined. MEA02.04 fully achieved PA 4.1 because it has been measured by identifying effective risk control constraints to support the implementation of the process, but has not run optimally according to the specified limits. MEA02.05 fully achieved PA 3.2 due to the definition of the guarantee standard, the independence of HRIS which has supported the implementation of an effective process. MEA02.06 fully achieved PA 3.2 because the company has carried out a risk assessment and measured the effectiveness of the implementation of the risk assessment. MEA02.07 fully achieved PA 3.2 because defined scope of scope and resource requirements to support the implementation of the HRIS and the standard is carried out effectively. MEA02.08 fully achieved PA 3.2 because measurements have been carried out measuring the extent to which the standard process of tracking corrective actions, evaluations and corrective actions from IT control and implemented effectively. After that, a gap analysis is performed and is described on the radar chart.

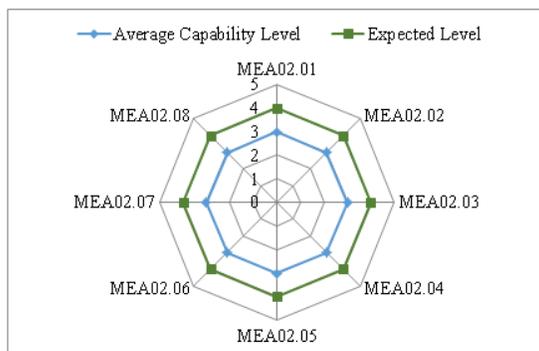


Figure 4: Radar Chart Capability Level MEA02

Based on Figure 4 Radar Chart Capability Level MEA02, it is known that the MEA02.01 gap analysis result is 1, with an average capability level of this process is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. MEA02.02 gap analysis results are 1, with an average level of capability of this process is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. MEA02.03 gap analysis results are 1, with an average level of capability of this process is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. MEA02.04 gap analysis results are 1, with an average capability level of this process

is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. MEA02.05 gap analysis results are 1, with an average level of capability of this process is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. MEA02.06 and MEA02.07 gap analysis results are 1, with an average level of capability of this process is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. MEA02.08 gap analysis results are 1, with an average level of capability of this process is 3 Established Process while the expected level to be achieved is level 4 Predictable Process. So overall, the MEA02 gap analysis where expected level 4 with the current level obtained 3, so that the gap owned is 1. After conducting a gap analysis, the authors then analyze the results of the gap analysis to make recommendations on the MEA02 process.

## 4.2 MEA02 Sub-process Recommendations

### 4.2.1 Recommendations Based on the MEA02.01 Sub-process

MEA02.01 Internal Controls Monitor has capability level 3 and has expected level 4. Then the recommendation for MEA02.01 sub-process to reach the expected level is to supervise internal IT control standards against the risk of implementing Human Resource Information Systems (HRIS) in order to provide confidence in operation so that it can run more effectively and efficiently.

### 4.2.2 Recommendations Based on the MEA02.02 Sub-process

MEA02.02 Review business process controls effectiveness has capability level 2 and has expected level 4. Then the recommendation for MEA02.02 sub-process to achieve expected level is to review the business processes of implementing the Human Resource Information System (HRIS) to control and predict risk by measuring the extent to which HRIS is managed by a well-regulated internal IT control process.

### 4.2.3 Recommendations Based on the MEA02.03 Sub-process

MEA02.03 Perform control self-assessments have capability level 3 and have expected level 4. Then the recommendation for MEA02.03 sub-process to reach expected level is to carry out risk self-assessment of HRIS regularly and regularly, with benchmarking of companies same industry. In addition, companies can predict the level of frequency of risks that may arise from the application of HRIS, whether at a low, medium or high level.

**4.2.4 Recommendations Based on the MEA02.04 Sub-process**

MEA02.04 Identify and report control deficiencies have capability level 3 and have expected level 4. Then the recommendation for MEA02.04 sub-process to reach the expected level is to carry out identification measurements by predicting the cause of the emergence of risk so that it can be used to ensure the implementation of processes that can support the achievement organization goals.

**4.2.5 Recommendations Based on the MEA02.05 Sub-process**

MEA02.05 Ensure that assurance providers are independent and qualified have capability level 3 and have expected level 4. Then the recommendation for MEA02.05 sub-process to reach the expected level is to measure the guarantee standards, rules of independence from the risk of implementing HRIS that support the implementation of the process effective periodically to produce a process that is stable and predictable according to defined limits.

**4.2.6 Recommendations Based on the MEA02.06 Sub-process**

MEA02.06 Plan assurance initiatives have a capability level 4 and have an expected level 4. Then the recommendation for the MEA02.06 sub-process is to maintain risk assessments and predict risk control actions arising from the application of HRIS.

**4.2.7 Recommendations Based on the MEA02.07 Sub-process**

MEA02.07 Scope assurance initiatives have capability level 2 and have expected level 4. Then the recommendation for MEA02.07 sub-process to achieve expected level is to measure HRIS collection and evaluation practices to produce a stable process and can predict the consequences of HRIS implementation.

**4.2.8 Recommendations Based on the MEA02.08 Sub-process**

MEA02.08 Execute assurance initiatives have capability level 3 and have expected level 4. Then the recommendation for MEA02.08 sub-process to achieve expected level is to measure the extent to which the standard process for tracking corrective actions, evaluations and corrective actions for HRIS risk is carried out periodically.

Table 7: SWOT Analysis

<b>SWOT</b>	<p style="text-align: center;"><b>Strength</b></p> <ul style="list-style-type: none"> <li>• Availability of SOPs from the application of the Human Resource Information System (HRIS).</li> <li>• Internal IT control over HRIS risk assessment is proceeding quite smoothly.</li> <li>• The company has understood and prioritized system risks towards the organization's goals.</li> <li>• Corrective actions by IT control over HRIS risks have been carried out regularly.</li> </ul>	<p style="text-align: center;"><b>Weakness</b></p> <ul style="list-style-type: none"> <li>• The process of identifying risks that arise is only in the low category and feels confident that the high risk category does not occur.</li> <li>• Implementation of corrective actions arising from the assessment and reporting of IT internal controls on the risk of implementing HRIS is only done in the present.</li> </ul>
<p style="text-align: center;"><b>Opportunity</b></p> <ul style="list-style-type: none"> <li>• Can benchmark with other similar companies that are growing rapidly.</li> <li>• Be consistent with the risk control measures of implementing HRIS.</li> <li>• Able to define risk opportunities that may arise from the application of HRIS.</li> </ul>	<p style="text-align: center;"><b>SO</b></p> <ul style="list-style-type: none"> <li>• Making plans, supervision and continuous improvement as in HRIS services that have been implemented.</li> <li>• Ensuring that all company employees understand the SOPs and the policies made by HRIS.</li> <li>• Documenting every activity and repairing risks in each HRIS process, such as recording every input, output and constraints in each activity.</li> </ul>	<p style="text-align: center;"><b>WO</b></p> <ul style="list-style-type: none"> <li>• Conduct analysis and documentation of all possible problems and risks at the low, moderate and high risk levels.</li> <li>• Planning for changes to risks arising from changes in the short, medium and long term.</li> <li>• Documenting all problems that have occurred, including problem solutions.</li> </ul>
<p style="text-align: center;"><b>Threat</b></p> <ul style="list-style-type: none"> <li>• Threats from external risks in the form of data theft and errors from human resources in using HRIS.</li> <li>• Impairment in the quality of internal performance or HRIS hardware.</li> <li>• The emergence of risk problems that are high risk and have an impact on HRIS implementation.</li> </ul>	<p style="text-align: center;"><b>ST</b></p> <ul style="list-style-type: none"> <li>• Improve security systems from internal and external risk control.</li> <li>• Control and supervise every activity using HRIS.</li> <li>• Determine the priority of HRIS risk improvement that must be achieved first.</li> </ul>	<p style="text-align: center;"><b>WT</b></p> <ul style="list-style-type: none"> <li>• Documenting every activity and change related to the use of HRIS.</li> <li>• Evaluate and improve each change.</li> </ul>

### 4.3 SWOT Analysis

SWOT analysis is used to separate strengths, weaknesses, opportunities and threats to IT services. Company performance can be determined by a combination of internal and external factors. This SWOT matrix can clearly illustrate how external opportunities and threats faced by the company can be adjusted to the strengths and weaknesses they have. Companies can review the implementation of enterprise architecture information systems from the old system to the new system in terms of improving the performance and business processes of the company [24]. This matrix can produce 4 sets of possible strategic alternatives. The alternative formulation of strategy is an alternative used by the company to run the business going forward. The following is a combination of matrix strategies derived from indicators and a combination of internal and external factors. Generally obtained as follows:

Based on Table 7 SWOT Analysis, the results of the SWOT analysis are obtained in terms of strengths, weaknesses, opportunities and risk threats that arise during the implementation of the Human Resource Information System in pharmaceutical companies. From the results of this analysis, it was also found that the formulation of alternative strategies in terms of the strength of opportunity, strength of threat, opportunity weakness and threat weakness. The formulation of this strategy can be used by pharmaceutical companies to carry out improvement strategies for handling risk problems that occur within the company.

The implication obtained from this research is to help the company's readiness in facing various possible disruptions or incidents that can lead to failure of the Human Resources Information System (HRIS). The risk analysis carried out in HRIS produces risk management principles and processes, in the form of a list of risks, risk levels, impacts, risk management and recommendations using the MEA02 domain from COBIT 5 and a SWOT analysis. This research ensures the achievement of company goals and objectives and provides sufficient knowledge about the risks of using HRIS. The results of this risk analysis can improve HRIS capabilities in increasing risk by taking advantage of opportunities that arise and anticipating emerging risks that will adversely affect HRIS operations, so that HRIS utilization can run well and as expected. Practical suggestions from this research is that it is hoped that the use of MEA02 can help manage risks from the application of HRIS, both internal and external risks.

### 5. CONCLUSION

The conclusions obtained from this study, among others, gap analysis MEA02 where expected level 4 with the current level obtained 3.5, so that the gap is 0.5. Companies need to do:

1. Oversight of internal IT control standards on the risks of implementing Human Resource Information Systems (HRIS) in order to provide confidence in operations so that they can run more effectively and efficiently.
2. Periodic and regular self-assessment of risk from HRIS, with benchmarking of the same industrial companies, so that they can predict the frequency of risks that may arise from the application of HRIS.
3. Risk analysis in HRIS needs to be done to deal with all the possibilities that result in HRIS failure. Increased use of HRIS leads to increased risk of implementing it.
4. The method used in HRIS risk analysis is COBIT 5 which focuses on the MEA02 domain for risk control in the planning process, setting and monitoring risk management standards in the application of HRIS.
5. The results obtained from this study are all the risks that have been previously described, these risks are at a low level. Risk analysis describes the frequency of occurrence, risk of risk impact of risk.
6. The recommendations made in this study are based on the COBIT 5 sub-domain MEA02 and SWOT Analysis.
7. From the SWOT analysis, several strategies are formulated so that the company is consistent and maximal in conducting risk analysis for the long term.
8. The implication of this research is to help the readiness of pharmaceutical companies in facing various possible disruptions or incidents that may result in the failure of the Human Resource Information System (HRIS).

### REFERENCES:

- [1] J. F. Andry, J. S. Suroso, and D. Y. Bernanda, "Improving quality of smes information system solution with ISO 9126," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 14, pp. 4610–4620, 2018.
- [2] J. F. Andry, H. Agung, and Y. Erlyana, "Management Information System for Order Fulfillment : a Case Study," *Proceeding 9th Int. Semin. Ind. Eng. Manag.*, no. May 2017, pp. 1–8, 2017.
- [3] J. F. Andry, B. Sebastian, "Conceptual Framework for Successful IT-Governance and

- BSC for Service Industry,” vol. 3, no. 5, pp. 1–6, 2018.
- [4] R. O. A. Khasawneh, “The Role and Importance Of Information Technology In Reducing the Risks of Information Technology Security in Government Units in The Light of Applying e-government governance The Role and Importance of Information Technology Governance in Reducing the Ri,” no. September, 2019.
- [5] S. Kosasi, “The Role of Information Technology in Organizational Development,” *Dinamik*, vol. 7, no. 1, pp. 93–104, 2018.
- [6] M. Ngafifi, “Technological Progress and Human Lifestyle in the Socio-Cultural Perspective,” *J. Pembang. Pendidik. Fondasi dan Apl.*, vol. 2, no. 1, pp. 33–47, 2015.
- [7] D. Rahmawati, “The Role of Information Technology in Auditing,” no. *Jurnal Bhirawa*, pp. 2337 – 523X, 2015.
- [8] H. Zafar, “Human resource information systems: Information security concerns for organizations,” *Hum. Resour. Manag. Rev.*, vol. 23, no. 1, pp. 105–113, 2017.
- [9] M. Wong, A. Setiawan, and A. Noertjahyana, “Audit of Human Resources Information Systems in Electronics Companies in Surabaya,” *J. Infra*, vol. 6, no. 1, pp. 151–155, 2018.
- [10] A. R. Yazid, “Analysis Of Human Resources Information Systems ( Case study on Aston Hotel Jember Jl . Sentot Prawirodirjo 88 , Jember ),” *J. Adm. Bisnis Brawijaya*, vol. 37, no. 2, pp. 97–103, 2016.
- [11] F. Hussein, Kertahadi, and Riyadi, “Implementation Of Human Resources Information System (Case Study on Service Company PT. Wiranas Laundry and Dry Cleaning Service),” *J. Adm. Bisnis*, vol. 10, no. 2, pp. 1–11, 2017.
- [12] B. A. Habeahan, A. R. Perdanakusuma, and W. H. Nugraha, “Analysis of Maturity of Information Technology Governance in the Internal Control Process Using the COBIT 5 Framework (Study in IT / FMS Department of PT. Macmahon Mining Service Batang Toru),” vol. 3, no. 5, 2019.
- [13] F. Ajismanto, “Analysis of the COBIT Framework 5 Process Domain in Worksheet Information Systems (Case Study: STMIK College, Palcomtech Polytechnic),” *CogITo Smart J.*, vol. 3, no. 2, p. 207, 2018.
- [14] T. S. Sukamto, “COBIT 5 As a Governance Framework TI.”
- [15] ISACA. Enabling Processes. ISACA, USA. 2012.
- [16] I. S. Sanjaya., N. Hiron., and A. P. Aldya., Governance Analysis Of Integrated Management Information System (SIMPADU) PNPM Mandiri Using COBIT Framework (Case Study: PNPM Mandiri Sukaresik District),” pp. 1–7.
- [17] R. E. Putri, “Model of Capability Assessment Process for Ti Risk Optimization Based on Cobit 5,” *Semin. Nas. Inform.* 2015, vol. 2015, no. November, pp. 252–258, 2015.
- [18] H. Purnomo, S. Fauziati, and W. W. Winarno, “Assessment of the Capability Level of Information Technology Governance Process With COBIT 5 In EDM Domain (Case Study in PT. Nusa Halmahera Minerals),” *Konf. Nas. Teknol. Inf. dan Komun. (KNASTIK 2016)*, no. November, pp. 63–69, 2016.
- [19] R. E. Putri, “Assessment of IT Governance Process Capabilities Based on DSS01 Process on COBIT Framework 5,” *J. CoreIT*, vol. 2, no. 1, pp. 41–54, 2016.
- [20] R. G. Mufti and Y. T. Mursityo, “Evaluation of Information Technology Security System Governance Using COBIT 5 Framework Focusing on APO13 and DSS05 Processes (Study at PT Martina Berto Tbk),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 12, pp. 1622–1631, 2017.
- [21] F. Muhafiih, Suprpto, and R. I. Rokhmawati, “Evaluation of Company Information Technology Resources Using COBIT 5 (Case Study: PT Krakatau Steel (Persero) Tbk),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 12, pp. 1687–1696, 2017.
- [22] H. Fakhurroja and Sopyan, “Information System Strategy Planning Using COBIT 5 Case Study Service and Development Bureau,” pp. 1–6, 2018.
- [23] J. F. Andry, Hartono, A. Chakir, “Assessment IT Governance of Human Resources Information System Using COBIT 5, *International Journal of Open Information Technologies*, vol. 8, no.4, pp. 59–63, 2018..
- [24] E. D. Madyatmadja. J. F. Andry, A. Chandra, “Blueprint Enterprise Architecture In Distribution Company Using Togaf,” *Journal of Theoretical and Applied Information Technology*, vol.98. no 12, pp. 2006–2016, 2020.