JOIV : Int. J. Inform. Visualization, 7(2) - June 2023 345-355

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Managing Information Technology Risks to Achieve Business Goals: A Case of Pharmaceutical Company

Luthfi Ramadani [a,*], Berlian Maulidya Izzati [a], Yosephine Mayagita Tarigan [a], Rosanicha [a]

[a] *Department of Information Systems, Telkom University, Bandung, Indonesia*
Corresponding author: [*]luthfi@telkomuniversity.ac.id

Abstract*—Extant literature has shown that sectoral characteristics play a critical role in business value creation through information technology (IT). Therefore, managing IT and its associated risks needs to consider specific industrial traits to understand the distinct business nature and regulations that shape IT-enabled business value creation. This study presents an in-depth analysis of business goals, IT processes, and IT risks in the case of a pharmaceutical company through which appropriate controls are designed to ensure business value creation through IT. Drawing on a case study of a pharmaceutical company in Indonesia, we found that managing IT risks in the pharmaceutical industry entails two main objectives: 1) ensuring compliance with external laws and regulations as well as internal policies, 2) supporting the optimization of business functions, processes, and costs. Throughout one year of engagement during the project, this study identified ten risks associated with the operation of business processes. Risks are dominated by moderate levels given the current state of controls and appetite, most of which emerge from the company's existing internal processes. Internal actors are involved in all risks, with most events occurring due to laws and regulations. Further, the study designs and elaborates IT risk controls by drawing from COBIT 5 Seven Enablers. Overall, IT risk management through cascading processes of analysis ensures the alignment of IT risk controls with achieving business goals in the pharmaceutical industry.

***Keywords*—Information technology risks; business-IT alignment; business value creation; pharmaceutical industry.**

Manuscript received 10 Jul. 2022; revised 10 Nov. 2022; accepted 19 Dec. 2022. Date of publication 30 Jun. 2023.
International Journal on Informatics Visualization is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

I. Introduction

Contemporary organizations worldwide are using information technology (IT) to transform their business, with most of them considering IT indispensable in day-to-day activities [1], [2]. However, the increasing reliance on information technology carries risks that stem from various sources or factors (Fig. 1) [3]. The failure to manage these IT risks could cost a company tangible and intangible losses. For instance, if product manufacturing data in a quality control division is unavailable or insufficient, the marketed product will be denied permission to be distributed to the public. Consequently, businesses need to perform IT risk management to ensure that their business goals are achievable [4], [5].

Performing IT risk management requires an in-depth understanding of the nature and dynamics of business sectors [6], [7]. Each business sector might have unique characteristics, ranging from the dynamics of competition, regulations, and internal and external contextual factors [8], [9]. In this regard, implementing the available IT risk management framework, like any IT governance framework, needs to be context-sensitive and cannot be taken for granted [10]–[12]. As such, literature has called for empirical studies to provide rich insights from diverse business sectors [6], [13] and enhance the overall understanding of the underlying business value creation process through IT [14]–[16].

This study responds to this call through an in-depth case study of IT risk management in the pharmaceutical industry. This study explores a State-Owned Enterprise pharmaceutical company in Indonesia, specializing in manufacturing a variety of medicine distributed across the nation. The study identifies business goals across the four balanced scorecards [17], IT capabilities to support business goals, and subsequent IT risks [18]. The study then assesses each risk to develop appropriate controls to be implemented by the company. Overall, this study provides rich empirical insights into the literature on IT risk management from the pharmaceutical industry [6] and the nation's contextual settings [19], [20]. The next section two describes the method used in this study. Section three provides the study's results which consist of the case study profile, the company's business goals, identification of IT capabilities, identification of IT risk, risk analysis, and risk control. Finally, section five provides the conclusion.

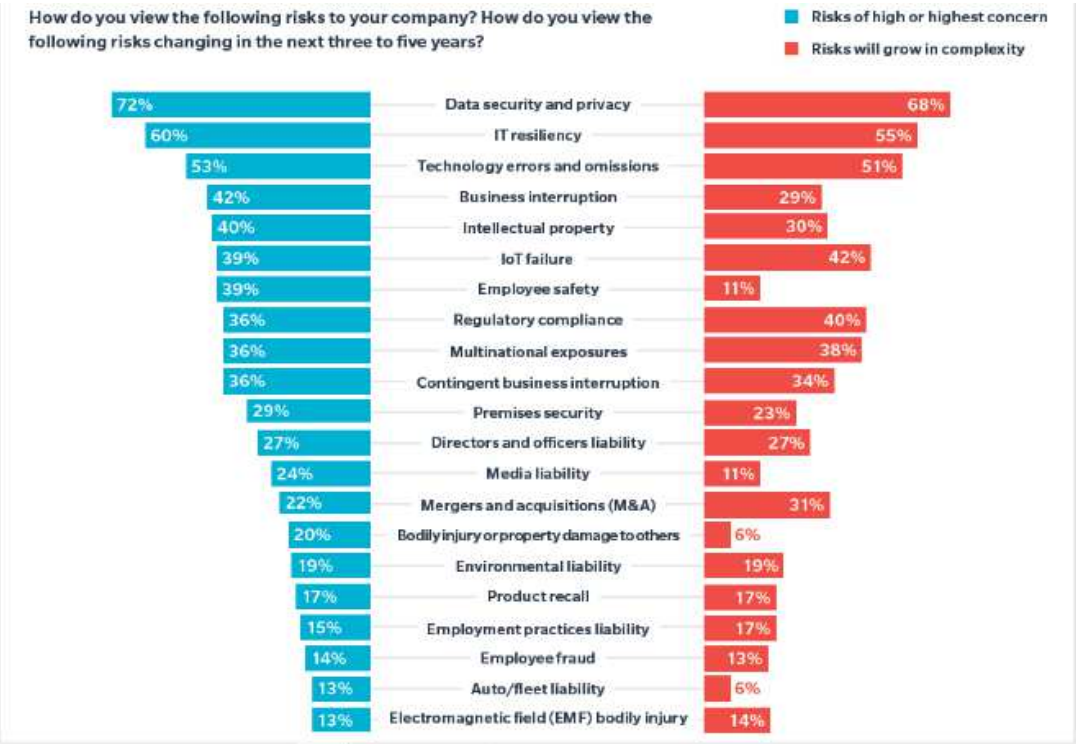

Fig. 1 The major concern of IT risks [3]

II. The Materials and Method

A. Theoretical Foundations

Risk is generally defined as the product of an event's probability and its consequence of unforeseeable events that could positively or negatively impact the project or enterprise's objectives [21], [22]. Risk management is a planned and structured process that aims to assist the project team in making the best decision possible at the right time by identifying, classifying, quantifying, and then managing and controlling risks. The objective is to maximize the project's value in terms of cost, time, and quality by balancing the input required to manage risks against the benefits of such action [4], [23].

COBIT 5 for Risk, a worldwide IT governance framework specifically intended for IT risk management, defines IT risk as business risk, more precisely, the risk to the enterprise associated with the use, ownership, operation, involvement, influence, and adoption of IT [24]. IT risk refers to IT-related events that may disrupt the business. IT risk occurs with an unknown frequency and magnitude and obstructs achieving strategic goals and objectives. IT risk is always present, regardless of whether an enterprise detects or recognizes it [22], [25].

Information technology risk management consists of five processes: 1) risk identification, 2) risk analysis, 3) risk prioritization, 4) risk response, and 5) risk monitoring. As shown in Fig. 2, COBIT 5 for risk includes seven enablers that assist businesses in achieving their business objectives. Each enabler in COBIT 5 for risk has the following objectives: 1) Principles, Policies, and Frameworks, 2) Processes, 3) Organizational Structure, 4) Culture, Ethics, Behavior, 5) Information, 6) Services, Infrastructure, and Applications and 7) People, Skills and Competencies [22].

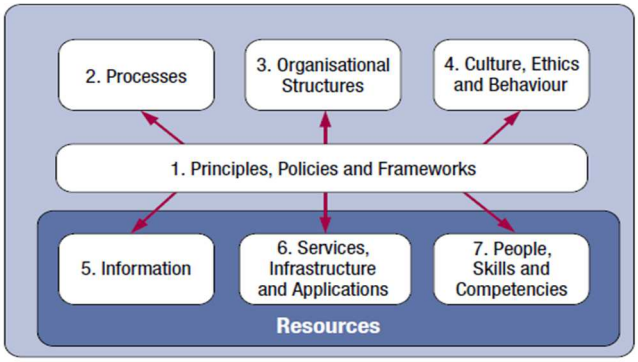

Fig. 2 COBIT's Seven Enablers [18]

While previous studies have examined IT risks in the manufacturing sector, few attempts have been made to investigate the pharmaceutical industry specifically. For example, Firdaus et al. [26] and Setyaningrum et al. [27] examined the risks associated with information technology in the manufacturing industry. Both organizations use COBIT 5 for risk management to assess information technology risk management. For instance, Firdaus et al. [26] identified the risks associated with using ERP-based SAP applications. They found that the company has corporate governance and risk management services. However, no management or team has been formed specifically for information technology risks, and not all information technology risks have been adequately documented and managed.

Similarly, Setyaningrum et al. [27] suggest that the use of information systems entails numerous risks, and the risks entail making work processes inefficient and lowering the company's quality. Another study by Thenu et al. [28] found that because information technology is used to support the business in the organization, IT-related risks can occur at any

time. Risk management is the best strategy for mitigating losses should this problem occurs.

B. Research Design and Data Collection

This study is designed as a qualitative case study [29]. We conducted the study in PharmaCo (pseudonym), one of the largest pharmaceutical companies in Indonesia. We focused on PharmaCo's core business in production and quality assurance. This study consists of four stages: 1) research planning and identification, 2) data collection, 3) risk identification and analysis, and 4) IT risk controls design.

Data collection methods include observation, interview, and document analysis. The primary sources are interviews and observation. The research participants are managers, assistant managers, and staff from the Quality Assurance and Regulatory Compliance Department of PharmaCo. Following COBIT 5, we identified Enterprise Goals (EG) and its subsequent IT-Related Goals and IT-Related Processes. The whole IT Risk Management activities consist of five stages:

1) Risk identification: In this step, risks are identified and listed to understand and determine the risk factors involved in a decision or project.

2) Risk analysis: Risk analysis is conducted based on its likelihood and probability according to company's ongoing risk management.

3) Risk prioritization: Risk prioritization is conducted based on company's risk appetite and categorized to low, medium, and high risk.

4) Risk response: Risk response is categorized to:

- Stop all potentially hazardous activities (Risk Avoidance).
- Take action to reduce the likelihood or impact (Risk Reduction).
- Take steps to transfer some or all of the risks to a third party, such as through insurance or outsourcing (Risk Sharing or Risk Transfer).
- Accepting the risk or failing to take risk-mitigation action (Risk Acceptance)

5) Risk monitoring: Once risk responses are established, the risk must be monitored and reviewed to see the possibility of changes that cause other risks to arise.

C. IT Risk Management Recommendation

We developed IT risks controls on PharmaCo's using COBIT's seven enablers. The existing condition is evaluated using the current process documents used during the risk analysis process. After determining the current situation, risk controls and recommendations are generated based on each of the existing risks, tailored to the requirements of each associated enabler.

III. Results and Discussion

A. Case Profile

PharmaCo (pseudonym) is a State-Owned Enterprise pharmaceutical company based in Indonesia that manufactures and distributes medicine and its derivative products across the nation. The company operates and manages its business processes using an ERP-based SAP application. Several risks associated with applications are frequently encountered, including less-than-optimal ERP operational technicalities, communication problems between users and servers, etc. PharmaCo has implemented guidelines based on the ISO 9001 framework to manage all types of risks that could disrupt business processes and result in losses.

PharmaCo has implemented its risk management procedures to ensure the security of its data and processes as a manufacturer of health products. The information technology risk management condition at PharmaCo's Quality Assurance Division requires research. The Quality Assurance Division utilizes the COBIT 5 risk framework, which is a risk management framework for information technology risk management. This study aimed to ascertain the state of information technology risk, conduct risk analysis, and make design recommendations for information technology risk management using COBIT 5 For Risk in the Quality Assurance Division of PharmaCo's Regulatory Compliance Division.

B. Aligning COBIT 5 Enterprise Goals with Enterprise Objectives of PharmaCo

Using a balanced scorecard, this section identifies the quality assurance and regulatory compliance divisions' enterprise goals (EG) to the COBIT 5 enterprise goals. The mapping of the COBIT 5 enterprise goals revealed that the enterprise goals aligned with the regulatory compliance section's quality assurance division based on workflow and risk. The selected enterprise goals are adapted to the current state of the QA Division of the Regulatory Compliance Division using balanced scorecard references. There are four Enterprise Objectives (EO) presented in Table 1. The company's strategic goal is mapped to Balance Scorecard (BSC) dimension, which consists of Finance, Customer, Internal and Learning and Growth dimension. The detail is provided in Table 2.

TABLE I
ENTERPRISE OBJECTIVES

No	Enterprise Objectives
EO1	Becoming the first-choice healthcare company that integrate and create sustainable value
EO2	Conducting business activities in the chemical and pharmaceutical industries, trade and distribution network, pharmaceutical retail and health services, and asset optimization.
EO3	Managing the company with Good Corporate Governance and operational excellence supported by professional Human Resources (HR).
EO4	Providing added value and benefits for all stakeholders.

TABLE II
IDENTIFICATION OF STRATEGIC GOALS WITH BALANCE SCORECARD

BSC Dimension	The Company Strategic Goal
Finance	• Reducing financial risk • Optimizing the cost structure
Customer	Maintain and improve quality by setting high-quality standards
Internal	Build a strong management system
Learning and Growth	Improving the quality of human resources

The Balanced Scorecard dimension is divided into seventeen enterprise goals. Tables 3, 4, 5 and 6 map each enterprise objective to the enterprise goals based on each BSC dimension. We only selected BSC enterprise goals that are related to enterprise objectives.

TABLE III
MAPPING BETWEEN ENTERPRISE OBJECTIVE (EO) AND ENTERPRISE GOAL IN FINANCIAL DIMENSION

EO	Financial	
EO1	EG3	The company applies the FMEA method to identify and address risks that may occur in products and processes, as well as RPN, which is a system for assessing risk levels
	EG5	The company implements a Whistleblowing System (WBS) to prevent acts of fraud by reporting violations and encouraging a culture of honesty and openness
EO2	EG2	The estimated period between the occurrence of an event and the identification of a loss is determined by management for each identified portfolio.
	EG4	The company refers to BPOM RI regulation No. 24 of 2017 concerning criteria and procedures for drug registration
EO3	EG1	PharmaCo's commitment to continuously improving the quality and competence of human resources
EO4	EG1	PharmaCo is always committed to increasing stakeholder involvement to increase shareholder value and other stakeholders.
	EG4	Conducting business activities based on CPOB, CPOTB, Halal Assurance System standards, ISO 9001:2015, ISO 14001:2015 and ISO 45001:2018

TABLE IV
MAPPING BETWEEN ENTERPRISE OBJECTIVE (EO) AND ENTERPRISE GOAL IN CUSTOMER DIMENSION

EO	Customer	
EO1	EG6	The Company establishes a specific work culture (core value)
	EG7	Conduct weekly or monthly meetings to discuss orders, timeliness of production, ability to carry out production, and approval of drug manufacture
	EG8	The company launched the PharmaCo mobile application which allows customers to obtain health services using only their gadgets
	EG9	Using the website based NDE (Nota Dinas Elektronik) application in decision making
EO2	-	-
EO3	EG6	Improving the Risk Culture through training and Professional Certification.
EO4	EG10	Conducting a customer satisfaction survey

TABLE V
MAPPING BETWEEN ENTERPRISE OBJECTIVE (EO) AND ENTERPRISE GOAL IN INTERNAL DIMENSION

EO	Internal	
EO1	EG11	PharmaCo applies end-to-end digitalization by developing Information Technology (IT) as one of the key enablers in realizing business strategy, including IoT, QR Code, Track and Trace
	EG13	The transformation from a pharmaceutical company to a healthcare company
	EG15	The company will rely on four pillars: research and development, automation and technology, human resources, and good corporate governance.
EO2	EG11	The company encourages the realization of sustainable growth with maximum achievement and makes efforts to optimize working capital
	EG13	Focusing on product development and upgrading production machines to make production more effective and efficient. PharmaCo focuses on producing traditional medicines, while the changes/additions are in the manufacture of cosmetics and drinking water.
EO3	EG11	Ensuring that all operational activities of the company are carried out by implementing aspects of Good Corporate Governance
	EG12	The company has an appropriate improvement program for each division.
	EG15	The company implements a GCG (Guidelines of Corporate Governance) system with the principles of leadership and good corporate governance built on Responsibility, Accountability, Fairness, and Transparency.

TABLE VI
MAPPING BETWEEN ENTERPRISE OBJECTIVE (EO) AND ENTERPRISE GOAL IN LEARNING AND GROWTH DIMENSION

EO	Learning and Growth	
EO1	EG17	The company encourages the realization of sustainable growth with maximum achievement and makes efforts to optimize working capital
EO2	EG16	PharmaCo already has an employee appraisal system that refers to performance as a step to motivate employees to give their best output.
	EG17	The Plant factory produces products related to COVID-19 such as favipiravir and remdesivir to increase people's immunity.
EO3	EG16	The Company already has a Talent Management program, namely an education and training program (Diklat) to improve and develop employees' competencies, skills, and attitudes to achieve PharmaCo's strategic goals. Improving the competency of human resources through professional training & certification programs to build a risk culture for all PharmaCo personnel and improve the implementation of an effective & efficient Risk Management System.
	EG17	The company encourages the realization of sustainable growth with maximum achievement and makes efforts to optimize working capital
EO4	-	-

After mapping the enterprise objective to BSC enterprise goals, we select the BSC enterprise goals that suit this study case. Four BSC enterprise goals are selected as shown in Table 7.

TABLE VII
SELECTED ENTERPRISE GOALS

EG	Selected Enterprise Goals
4	Compliance with external laws and regulations
11	Optimization of business process functions
12	Optimization of business process costs
15	Compliance with internal policies

D. Mapping of IT-Related Goals at PharmaCo

The mapping of selected Enterprise Goals and IT Related Goals resulted in eleven goals, as shown in Table 8.

TABLE VIII
THE SELECTED IT-RELATED GOALS

ITG	IT-related goals
1	Alignment of IT and business strategies
2	IT compliance and support for business compliance with external laws and regulations
4	Manage business risks associated with information technology
6	Transparency regarding the costs, benefits, and risks associated with information technology
7	Delivering information technology services following business requirements
8	Adequate use of application, information, and technology solutions
9	IT can adapt to changes quickly
10	Security and information, infrastructure, and applications
11	Optimization of IT assets, resources, and capabilities
12	Utilization and support of business processes through the integration of applications and technology
15	IT compliance with internal policies

E. Mapping of IT-Related Process

The next step is to identify organizational processes associated with IT-Related Goals. We identified six IT Processes related to Quality Assurance in PharmaCo, which are presented in Table 9. The total score is calculated based on the 'primary value' based on the mapping between IT Related Goals and IT Processes. This step identifies IT-related processes that are highly related to internal-external compliance and internal processes in PharmaCo.

TABLE IX
IT-RELATED PROCESS PRIORITIZATION

No	IT Process		Total Score
1	EDM01	Ensure Governance Framework Setting and Maintenance	2
2	EDM02	Ensure Benefits Delivery	3
3	**EDM03**	**Ensure Risk Optimisation**	**4**
4	EDM04	Ensure Resource Optimisation	2
5	EDM05	Ensure Stakeholder Transparency	2
6	**APO01**	**Manage the IT Management Framework**	**5**
7	APO02	Manage Strategy	1
8	APO03	Manage Enterprise Architecture	3
9	APO04	Manage Innovation	3
10	APO05	Manage Portfolio	1
11	APO06	Manage Budget and Costs	1
12	APO07	Manage Human Resources	1
13	APO08	Manage Relationships	2
14	APO09	Manage Service Agreements	1
15	APO10	Manage Suppliers	3
16	APO11	Manage Quality	1
17	**APO12**	**Manage Risk**	**3**
18	APO13	Manage Security	3
19	BAI01	Manage Programmes and Projects	1
20	BAI02	Manage Requirements Definition	2
21	BAI03	Manage Requirements Definition	1
22	BAI04	Manage Availability and Capacity	2
23	BAI05	Manage Organisational Change Enablement	1
24	**BAI06**	**Manage Changes**	**3**
25	BAI07	Manage Change Acceptance and Transitioning	2
26	BAI08	Manage Knowledge	1
27	BAI09	Manage Assets	2
28	BAI10	Manage Configuration	2
29	DSS01	Manage Operations	3
30	DSS02	Manage Service Requests and incidents	2
31	DSS03	Manage Problems	3
32	DSS04	Manage Continuity	2
33	DSS05	Manage Security Services	3
34	DSS06	Manage Business Process Controls	2
35	**MEA01**	**Monitor, Evaluate, and Assess Performance and Conformance**	**4**
36	**MEA02**	**Monitor, Evaluate, and Assess the System of Internal Control**	**3**
37	MEA03	Monitor, Evaluate, and Assess Compliance with External Requirements	2

F. Risk Identification

Risk identification is a process of finding, recognizing, and recording risks. Risk identification aims to identify events or situations that may affect the achievement of organizational goals, including causes and sources of risk, descriptions of risk events, and their impact on organizational goals. Identification is conducted by developing risk scenarios based on the positive and negative sides of the risk. We identified a total of ten risks, which are presented in Table 10. Detailed risk identification, including actor, threat type, event, asset, and timing, is presented in Table 11.

TABLE X
RISK IDENTIFICATION

ID Risk	Risk	Process Domain
QA 01	Error in making regulatory documents	APO02, MEA02
QA 02	Error in distributing regulatory documents	APO02, DSS06
QA 03	Regulatory documents have not been approved but are already in use	APO02, EDM03
QA 04	Uncontrolled change	BAI06
QA 05	Changes that have been submitted are not verified	APO02, BAI02, BAI07
QA 06	Exceptions to applicable regulations occur frequently	MEA01
QA 07	Customer complaints that are not following the established SLA	APO09, DSS02
QA 08	Loss of data/documents due to an error in the application	BAI09, APO13

ID Risk	Risk	Process Domain
QA 09	The work process is not following the established procedures.	APO02, DSS06
QA 10	Too much workload	APO07

TABLE XI
RISK IDENTIFICATION BASED ON ACTOR, THREAT TYPE, EVENT, ASSET, AND TIMING

ID Risk	Actor	Threat Type	Event	Asset	Timing
QA 01	Internal	Error	Rules and Regulation	Information	Time Lag
QA 02	Internal	Error	Rules and Regulation	Process	Time Lag
QA 03	Internal	Failure	Rules and Regulation	Process	Duration
QA 04	Internal	Failure	Rules and Regulation	Process	Timing Occurrence
QA 05	Internal	Failure	Rules and Regulations, modification	Process, Information	Timing Occurrence
QA 06	Internal	Failure	Rules and Regulation, Ineffective execution	Process	Duration
QA 07	Internal	Failure, Error	Rules and Regulation, Ineffective execution	Process	Duration
QA 08	Internal	Error, Malicious	Interruption, Application	IT Infrastructure	Detection
QA 09	Internal	Failure	Rules and Regulation	Process	Duration
QA 10	Internal	Failure	People and Skill	People and Skill	Duration

G. Risk Scenario

IT risk scenario is a description of an event related to IT that can cause a business impact according to the possible time of the risk occurrence. Risk scenarios consist of two types based on whether the impact is positive scenarios or negative scenarios. The positive scenario represents the impact should the risk not occur, thus leading to smooth and optimal business processes. On the other hand, the negative scenario represents the impact should the risk occurs, resulting in disruption to business processes. Scenarios are created for each type of risk. Table 12 presents the risk scenarios at PharmaCo.

TABLE XII
RISK SCENARIO

ID	Risk Scenario	
	Positive	Negative
QA 01	Risk handling can be done quickly and precisely so that documents are immediately verified.	The document preparation was not to the applicable directives and regulations in that so many errors were found, which could result in the distribution permit not being issued.
QA 02	The regulatory compliance department revises documents in a timely manner.	The shared document is not the latest revised document but is urgently needed.
QA 03	The use of the document has been approved by the regulatory compliance department so that the document can be distributed immediately.	The use of documents that regulatory compliance parties have not verified makes the legality of documents questionable.
QA 04	Every time there is a change in processes, tools, materials or other things, each division notifies the regulatory compliance department.	Changes made without confirmation will cause business processes to go out of control and may impact other divisions.
QA 05	The handling of changes is carried out appropriately and immediately verified so that these changes can be implemented immediately.	Changes that occur are not monitored. This can impede the work of related divisions and have an impact on these changes.
QA 06	Handling of violations runs smoothly in accordance with procedures so as not to impede workflow.	There are repeated violations of the rules
QA 07	Customers can submit complaints which will then be resolved by regulatory compliance in a timely manner.	The number of customer complaints is because they are not handled immediately, so the service business process becomes impeded.
QA 08	Application systems and databases are very effective, and maintenance is often carried out.	Data that has been stored is lost due to an application system error, so data backup must always be done.
QA 09	The workflow is in accordance with fixed procedures so that the entire process is properly recorded.	Procedures are still not followed properly, which causes not all procedures to be carried out on time.
QA 10	The use of IT can be used to do various jobs.	Many job descriptions do not match the work being done, which can cause a process to take more time.

TABLE XIII
RISK MATRIX

Frequency	Impact				
	Very low	Low	Moderate	High	Very high
Very high					
High					
Moderate			QA03, QA04, QA05, QA07		
Low			QA01, QA02,	QA08	

Frequency	Impact				
	Very low	Low	Moderate	High	Very high
Very low			QA06, QA10		

C. Risk Assessment Criteria

The risk criteria are a standard measure of the probability, frequency, or likelihood of the occurrence of a certain risk as well as the consequences that may result should the risk

occurs. Table 13 presents a matrix of risk impact and probability, while criteria for probability and impacts are presented in Tables 14 and 15. The level of impact is assessed through FMEA (Failure Mode Effect Analysis) method in that we assess the current controls implemented in the company and the stakeholders' risk appetite.

TABLE XIV
PROBABILITY CRITERIA

Probability	Description
Very low	The threat occurred in only one batch and never happened again
Low	Threats occur once a year or only in one batch
Moderate	Threats happen once every three months
High	Threats occur once a week or in certain batches
Very high	Threats occur every day or every batch

TABLE XV
IMPACT CRITERIA

Severity	Patient / Safety Impact	Compliance Impact	Process Impact
Very high	Failure that leads to death	Revocation of business license, product recall	Product loss or failure
High	Failure that causes serious injury	Get a warning letter	Product re-process
Medium	Failure that causes minor injury	Can be a finding at the time of the audit	Late product release
Low	A failure that does not cause any harm	No effect on compliance	There is an effect on the process, but it does not affect the quality of the product
Very low	A failure that does not cause any harm	No effect on compliance	No influence on the process

D. Risk Analysis

Further analysis is conducted to relate the identified risks with organizational processes. Table 16 presents the risk analysis at PharmaCo.

TABLE XVI
RISK ANALYSIS

ID	Risk	Probability	Impact	Risk Level	Process Domain
QA 01	Error in making regulatory documents	Low	Moderate	Low	APO02, MEA02
QA 02	Error in distributing regulatory documents	Low	Moderate	Low	APO02, DSS06
QA 03	Regulatory documents have not been approved but are already in use	Moderate	Moderate	Moderate	APO02, EDM03
QA 04	Uncontrolled change	Moderate	Moderate	Moderate	BAI06
QA 05	Changes that have been submitted are not verified	Moderate	Moderate	Moderate	APO02, BAI02, BAI07
QA 06	Exceptions to applicable regulations occur frequently	Low	Moderate	Moderate	MEA01
QA 07	Customer complaints that are not following the established SLA	Moderate	Moderate	Moderate	APO09, DSS02
QA 08	Loss of data/documents due to an error in the application	Low	High	Low	BAI09, APO13
QA 09	The work process is not following the established procedures.	Low	Moderate	Low	APO02, DSS06
QA 10	Too much workload	Low	Moderate	Low	APO07

E. Risk Prioritization and Response

Risk prioritization is conducted to classify the risk level and identify the risk responses for each risk according to organizational processes. Risk responses are determined based on four risk management options: accept, mitigate, transfer, or avoid. Table 17 presents the results of risk prioritization and response.

TABLE XVII
RISK PRIORITIZATION

ID	Risk Level	Risk Category	Response	Process Domain
QA 05	Moderate	Regulatory Compliance)	Avoid	APO02, BAI02
QA 03	Moderate	Regulatory Compliance	Mitigate	APO02, EDM03, APO12
QA 04	Moderate	Regulatory Compliance	Mitigate	BAI06, BAI07
QA 06	Moderate	Regulatory Compliance	Mitigate	MEA02
QA 07	Moderate	Regulatory Compliance	Mitigate	APO09, DSS02
QA 02	Low	Regulatory Compliance	Mitigate	APO02, DSS06, APO12
QA 01	Low	Information (data breach: damage, leakage, and access)	Mitigate	APO02, MEA02, APO12
QA 08	Low	Software	Mitigate	BAI09, DSS05
QA 09	Low	Regulatory Compliance	Mitigate	DSS06
QA 10	Low	IT expertise and skills	Accept	APO07

After risk prioritization, a mapping between the alignment of strategies and the risk approach is performed to determine the process domain that best fits the overall risk. This step aims to determine the processes that need to be managed related to IT risk management. The risk priority ranking is summarized in Table 18.

TABLE XVIII
PROCESSES DOMAIN BASED ON RISK PRIORITIZATION

Strategic Alignment	Risk Approach
EDM03, APO01, **APO12,** MEA01, MEA02, **BAI06**	**EDM03**, APO02, APO07, MEA02, DSS06, BAI02, **BAI06, APO12**, APO09, DSS02, BAI09, DSS05

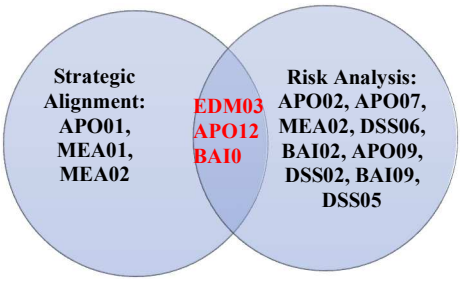

Fig. 3 The intersection of Process Domain

Figure 3 shows that the priority/main process domains for IT risk management at PharmaCo are EDM03 Ensure Risk Optimization, APO12 Manage Risk, and BAI06 Manage Changes. Each of these processes is briefly discussed next.

EDM03: Ensure Risk Optimization is one of the five domain processes of Evaluate, Direct, and Monitor.EDM03 focuses on stakeholder-related objectives to ensure that enterprise risk categories and tolerances are understood, articulated, and communicated and that risks to enterprise value associated with the use of IT are identified and managed. In addition, EDM03 ensures that the company's IT-related risks do not exceed its risk appetite and risk tolerance, the impact of IT risks on company value is identified and managed, and the potential for failure is minimized [30].

APO12: Manage Risk is one of 13 process domains associated with the Align, Plan, and Organize (APO) management areas. APO12 identifies, assesses, and mitigates IT-related risks within tolerance levels established by the company's executive management. In addition, APO12 integrates IT-related enterprise risk management with overall ERM, balancing the costs and benefits of IT-related enterprise risk management. In addition, all company activities have risk exposures, which means that the company's stakeholder approach to risk needs to be written down to show how the company will deal with the risks it faces.

BAI06: Manage Changes is a process that manages all changes in a controlled manner, including standard changes and emergency maintenance related to business processes such as standard change procedures, impact assessment, authorization, emergency change, tracking, and documentation. The goal of the BAI06 process is to make changes to the business quickly and make sure there aren't any risks that could harm the environment.

F. Designing IT Risk Management at PharmaCo

Assessment of existing conditions is carried out based on documents related to the current risk mitigation strategy. The design of IT Risk Controls for PharmaCo is based on COBIT's seven enablers that emerge from three perspectives:

- People: Organization, people/skill/competencies, culture
- Process: principle, policies, and frameworks, process
- Technology: information, services/infrastructure, and application

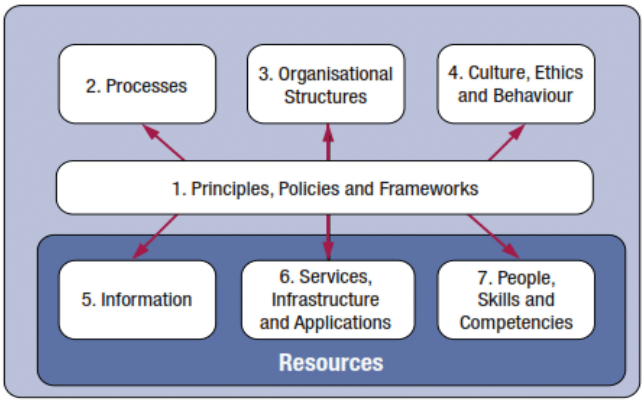

Fig. 4 COBIT 5 Seven Enablers

1) Principles, Policies, and Frameworks:

- Quality Manual: A quality manual document is created to define quality management (GMP, CPOTB, ISO 9001:2015, and Halal Assurance System) and to demonstrate how the company implements these standards.
- PharmaCo Quality Policy Document
- PharmaCo Quality Goal Document
- PharmaCo Quality Plan Document
- Regulation of the Head of the Indonesian Food and Drug Supervisory Agency No. 24 of 2017 Concerning Drug Registration Criteria and Procedure
- Regulation of the Head of the Indonesian Food and Drug Supervisory Agency No. HK.00.05.3.1818 of 2005 on Bioequivalence Testing Guidelines
- CPOB Manual 2018
- CPOTB Manual 2011

2) Processes:

Standard Operating Procedures (SOP) for Risk Assessment: Procedures used as guidelines in quality risk management for all systems, processes, tools, and facilities used and implemented at PharmaCo. The forms and templates used in this SOP are:

- Ishikawa Diagram Templates
- FMEA Form
- Risk matrix
- Risk Assessment List Form

SOP for Regulatory Management: This document aims to ensure that the registration documents sent are correct and complete. Some of the documents that need to be prepared for registration documents are:

- Administrative documents, product information, and labels
- Quality document
- Non-Clinical Documents
- Clinic Documents

SOP for Change Control: Procedures to prevent uncontrolled changes

*3) Organizational Structure (*Role and Responsibility):

- Assistant Manager Quality Assurance (R). Assistant Manager Quality Assurance is responsible for

reviewing and approving procedures related to SOPs for Risk Assessment, Regulatory Management, and Quality Manuals.

- Plant Manager (A). The Plant Manager is responsible for checking, approving, and ensuring the SOP is executed properly, ensuring that the management system complies with applicable standards.
- Supervisor Compliance (I/ R). Supervisor Compliance is responsible for compiling, reviewing periodically, and ensuring that the SOP for risk assessment is carried out consistently, properly, and correctly. The supervisor of each sub-section is also responsible for carrying out risk management following the established Risk Assessment SOP.

4) Culture, Ethics, and Behavior: Existing behavior and related risk management are carried out based on the risk appetite that has been set in the Risk Assessment SOP

5) Information

SOP for Risk Assessment. The process that occurs in risk assessment is the process of risk assessment, risk control, and risk assessment using the Ishikawa Diagram tools. The results of the risk assessment are prepared according to the FMEA form. After the risk assessment is completed, it is submitted to the Assistant Manager of Quality Assurance for approval and documentation of the risk assessment list form and FMEA form.

SOP for Regulatory Management. In the regulatory procedure, there is a process of preparing and sending registration documents. This process produces an output, namely a Memo of product batch number and a Drug Registration Document, which will be submitted to the Head Office Regulatory Section, which consists of:

- Change Proposal Form
- Change Approval Form
- Change Approval Verification Form
- Risk Assessment Form
- Customer Satisfaction Survey Form

In terms of compliance with the Pharmaceutical Industry Quality System standards, GMP, CPOBT, ISO 9001:2015, and the Halal Assurance System is communicated by letter, email, or other communication, confirmed with the relevant customer, and documented.

6) Services, Infrastructure, and Applications: All documents are managed in PharmaCo's application on the E-Document module.

7) People, Skills, and Competencies: In improving the knowledge and abilities of all employees, PharmaCo has two main sources, namely:

- Internal resources: such as training, expert feedback, training materials, intellectual property, and internal collaboration.
- External sources: such as standards, academics, seminars, customer and supplier information, and internet information.
-
- The company conducts HR development by:
- Find out what skills employees need to do work that affects the quality of the product.
- Put in place training and induction programs to ensure that competency requirements are met.
- Assess the effectiveness of the actions taken following the training.
- Gather information on personnel competency.
- Conduct awareness building on the company's quality objectives.

G. Design of IT Risk Management

At this stage, recommendations are developed based on the data analysis results and the business's current state, as categorized by the seven enablers. Recommendations focus on risks that have been mitigated and the portion of the system that has not yet reached its optimal state or has gaps that require improvement. Table 19 presents the recommendations for IT risk management at PharmaCo.

TABLE XIX
DESIGN OF IT RISK MANAGEMENT AT PHARMACO

ID	Risk	Control Recommendation Based on Enabler	
QA01	Error in making regulatory documents	**Principles, Policies, and Frameworks**	• Adding and detailing related SOPs for Regulatory Procedures, how the flow in document creation works and what policies are needed so that document creation can be carried out correctly • The Quality Manual and Risk Assessment SOP documents do not explain the policy that requires document verification before use, so the recommendation is to make a policy regarding the use of the documents that must be approved first. • Detailed work process flow, namely SOP for Risk Assessment and SOP for Regulatory Management, so that they can be carried out according to the provisions of the procedure
QA02	Error in distributing regulatory documents	**Processes**	All applicable process procedures, including SOP for Risk Assessment, Regulatory Management, and Change Control, are proposed. The design of controls for each of the processes includes: • Develop and establish a drug registration process in Regulatory Management • Impact of changes in the Change Control SOP
QA03	Regulatory documents have not been approved but are already in use		Based on the process domain related to risk, IT risk controls consist of: • APO02: An IT risk management strategy must be defined and aligned with the Enterprise Risk Management (ERM) approach through Risk Management Strategy outputs. • MEA02: Carrying out the internal control

ID	Risk	Control Recommendation Based on Enabler	
			• DSS06: Maintain control over business processes and IT assets. • EDM03: Ensure risk optimization • BAI07: Determine who has access to risk management documents.
QA09	The work process does not follow the established procedures	**Services, Infrastructure, and Applications**	The regulation module is added to the existing application to categorize related documents according to the division and make attachments in the submodules.
QA04	Uncontrolled change	**Processes**	SOP Control: Adding details of what changes must be reported and what the references are. BAI06: Manage all changes in a controlled manner, including standard changes and emergency maintenance related to business processes. Such as standard change procedures, impact assessment, emergency changes, tracking, and documentation.
		Services, Infrastructure, and Applications	It added change updates in the application dashboard so that all employees can know the changes made in real-time and up to date.
QA06	Exceptions to applicable regulations occur frequently	**Culture, Ethics, and Behavior**	To conduct routine socialization in offline and online seminars to discuss regulations and properly handle irregularities.
QA07	Customer complaints that are not following the established SLA	**Information**	• To update customer satisfaction survey documents tailored to the conditions and relationships between PharmaCo and customers. • To process information related to customer complaints through the information system
		Services, Infrastructure, and Applications	To add the Customer Complaints module to the Deviation Control & Customer Complaints sub-section to be accessed in the application and do checklists and updates related to handling customer complaints.
QA08	Loss of data/documents due to an error in the application	**Processes**	Recommendations based on the process domain related to risk: • BAI09: manage assets throughout their life cycle to ensure they provide value at an optimal budget, are physically recorded and protected, and are critical to supporting existing service capabilities. Manage software licenses to ensure optimal numbers and software installed following the agreement. • DSS05: complies with security policies regarding its own IT assets.
		Services, Infrastructure, and Applications	Regularly perform application maintenance. • Change passwords periodically to prevent other parties from seeing internal data. • Each division's backup data or documents use Drive, Flash disk, and Hard Disk.

IV. Conclusion

This research identifies ten IT risks, mainly related to the company's goals on regulatory compliance and internal process optimization. All risks have internal actors, with most events occurring due to rules and regulations factors. Most of the identified risks are dominated by a moderate level of risk. IT risk controls are designed based on various aspects of the seven enablers and customized for each risk. In terms of process, IT risk controls include details on creating work process flows and the enabling principles, policies, and framework sections. In terms of Services, Infrastructure, and Applications, IT risk controls include acquiring more efficient document storage and a dashboard for tracking changes. This entails storing data and processes about customer complaints in an application system in information technology. Finally, in terms of Culture, Ethics, and Behavior, IT risk controls include training and skill improvement related to rules and regulations to avoid overlapping or repeated abnormality/violation.

References

[1] K. K. Ganju, P. A. Pavlou, and R. D. Banker, "Does information and communication technology lead to the well-being of nations? A country-level empirical investigation," *MIS Q.*, vol. 40, no. 2, pp. 417–430, 2016.

[2] P. C. Verhoef *et al.*, "Digital transformation: A multidisciplinary reflection and research agenda," *J. Bus. Res.*, vol. 122, no. September 2019, pp. 889–901, 2021, doi: 10.1016/j.jbusres.2019.09.022.

[3] Marsh&McLennan, "A New Definition of Catastrophic Risk: Technology Industry Risk Study 2020," 2020.

[4] W. A. Cram, M. K. Brohman, and R. B. Gallupe, "Information systems control: A review and framework for emerging information systems processes," *J. Assoc. Inf. Syst.*, vol. 17, no. 4, pp. 216–266, 2016, doi: 10.17705/1jais.00427.

[5] A. Yeow, C. Soh, and R. Hansen, "Aligning with new digital strategy: A dynamic capabilities approach," *J. Strateg. Inf. Syst.*, vol. 27, no. 1, pp. 43–58, 2018, doi: 10.1016/j.jsis.2017.09.001.

[6] H. C. Chae, C. E. Koh, and K. O. Park, "Information technology capability and firm performance: Role of industry," *Inf. Manag.*, vol. 55, no. 5, pp. 525–546, 2018, doi: 10.1016/j.im.2017.10.001.

[7] N. Melville, K. L. Kraemer, and V. Gurbaxani, "Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value," *MIS Q.*, vol. 28, no. 2, pp. 283–322, 2004.

[8] K. J. Dooley and A. H. Van de Ven, "Explaining Complex Organizational Dynamics," *Organ. Sci.*, vol. 10, no. 3, pp. 358–372, 1999.

[9] M. D. Stoel and W. A. Muhanna, "IT capabilities and firm performance: A contingency analysis of the role of industry and IT capability type," *Inf. Manag.*, vol. 46, pp. 181–189, 2009, doi: 10.1016/j.im.2008.10.002.

[10] A. E. Brown and G. G. Grant, "Framing the Frameworks: A Review of IT Governance Research," *Commun. Assoc. Inf. Syst.*, vol. 15, no. May, 2005, doi: 10.17705/1cais.01538.

[11] A. Tiwana and S. K. Kim, "Discriminating IT Governance," *Inf. Syst. Res.*, vol. 26, no. 4, pp. 656–674, 2015, doi: 10.4018/978-1-60566-026-4.ch315.

[12] V. Sambamurthy and R. W. Zmud, "Arrangements for information technology governance: A theory of multiple contingencies," *MIS Q.*, vol. 23, no. 2, pp. 261–290, 1999, doi: 10.2307/249754.

[13] J. E. Gerow, J. B. Thatcher, and V. Grover, "Six types of IT-business strategic alignment: An investigation of the constructs and their

measurement," *Eur. J. Inf. Syst.*, vol. 24, no. 5, pp. 465–491, 2015, doi: 10.1057/ejis.2014.6.
[14] P. Weill, "Don't just lead, govern: How top-performing firms govern IT," *MIS Q. Exec.*, vol. 8, no. 1, pp. 1–21, 2004, doi: 10.2139/ssrn.664612.
[15] R. Kohli and V. Grover, "Business Value of IT: An Essay on Expanding Research Directions to Keep up with the Times," *J. Assoc. Inf. Syst.*, vol. 9, no. 1, pp. 23–39, 2008.
[16] V. Grover and R. Kohli, "Cocreating IT value: New capabilities and metrics for multifirm environments," *MIS Q.*, vol. 36, no. 1, pp. 225–232, 2012.
[17] R. S. Kaplan and D. P. Norton, "Using the Balanced Scorecard as a Strategic Management System," *Harv. Bus. Rev.*, vol. Jan-Feb, pp. 75–85, 1996.
[18] ISACA, *COBIT 5: A business framework for the governance and management of enterprise IT COBIT 5*. ISACA, 2012.
[19] L. Ramadani and A. Almaarif, "Considering context in information systems research: Understanding the conditions of developing country scholarship," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 88, no. 1, pp. 1–17, 2022, doi: 10.1002/isd2.12200.
[20] C. Avgerou, "Contextual explanation: Alternative approaches and persistent challenges," *MIS Q.*, vol. 43, no. 3, pp. 977–1006, 2019, doi: 10.25300/MISQ/2019/13990.
[21] K. Srinivas, "Process of Risk Management," *Perspect. Risk, Assess. Manag. Paradig.*, pp. 0–16, 2019, doi: 10.5772/intechopen.80804.
[22] ISACA, *COBIT 5 for Risk*. ISACA, 2013.
[23] T. Kude, M. Lazic, A. Heinzl, and A. Neff, "Achieving IT-based synergies through regulation-oriented and consensus-oriented IT governance capabilities," *Inf. Syst. J.*, vol. 28, no. 5, pp. 765–795, 2018, doi: 10.1111/isj.12159.
[24] S. De Haes, W. Van Grembergen, and R. S. Debreceny, "COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities," *J. Inf. Syst.*, vol. 27, no. 1, pp. 307–324, 2013, doi: 10.2308/isys-50422.
[25] Z. Alreemy, V. Chang, R. Walters, and G. Wills, "Critical success factors (CSFs) for information technology governance (ITG)," *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 907–916, 2016, doi: 10.1016/j.ijinfomgt.2016.05.017.
[26] N. Z. Firdaus and Suprapto, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT . Petrokimia Gresik)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 1, pp. 1–10, 2018.
[27] N. D. Setyaningrum, Suprapto, and A. Kusyanti, "Tampilan Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 (Studi Kasus : PT. Kimia Farma (Persero) Tbk – Plant Watudakon)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 1, pp. 143–152, 2018.
[28] P. P. Thenu, A. F. Wijaya, C. Rudianto, U. Kristen, and S. Wacana, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus: PT Global Infotech)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, Feb. 2020, doi: 10.33557/BINAKOMPUTER.V2I1.799.
[29] R. K. Yin, "Case Study Research and Applications Design and Methods Sixth Edition," 2018.
[30] M. Majdalawieh and J. Gammack, "'An Integrated Approach to Enterprise Risk: Building a Multidimensional Risk Management Strategy for the Enterprise,'" *Int. J. Sci. Res. Innov. Technol.*, vol. 4, no. 2, pp. 2313–3759, 2017.