Risk Management Analysis Using COBIT 4.1 at Vehicle Testing Management Information System

http://dx.doi.org/10.28932/jutisi.v7i1.3419
Riwayat Artikel
Received: 19 Februari 2021 | *Final Revision*: 14 Maret 2021 | *Accepted*: 16 Maret 2021

Resad Setyadi✉#1, Septian Anggoro#2

#*Program Studi Sistem Informasi, Fakultas Informatika*
Institut Teknologi Telkom Purwokerto
DI Panjaitan No 128 Purwokerto, Central Java
1resad@ittelkom-pwt.ac.id
217103040@ittelkom-pwt.ac.id

Abstract — **The role of information technology in an organization is growing so fast. Vehicle Testing of Management Information System (VTMIS) is a system that uses information technology to serve users in motor vehicle administration in the Banyumas transportation service area. VTMIS at the Banyumas Transportation Department is an integrated information system for the motor vehicle testing process starting from the registration process, levy payment, and vehicle testing. The purpose of this study is to analyze the risk management at VTMIS in Banyumas Transportation Department using Control Objective for Information and Related Technology (COBIT 4.1) domain Plan and Organize (PO) 9. COBIT 4.1 is a framework for analyzing and ensuring information technology aligns with business management by calculating maturity levels. The data analysis results from the PO9 domain show that VTMIS risk management has a maturity level of 3.46. The maturity level of VTMIS at the Banyumas Transportation Department is at level 3, namely defined, meaning that procedures are in a position of standardization, documentation, and individual communication. The recommendation for VTMIS at the Banyumas Transportation Department needs to carry out risk management in a structured, massive and integrated manner.**

Keywords— **control objective for information and related technology; maturity level; plan and organize; risk management; vehicle testing of management information system.**

I. PENDAHULUAN

Information technology (IT) is essential for government institutions, especially during the COVID-19 pandemic situation [1]. Information technology (IT) is necessary for all work and human mobility activities [2]. IT provides many positive benefits, including solutions for companies in operations and business, enabling the company to grow, making it competitive with other companies [3], [4]. However, IT also negatively impacts virus attacks, data hacking, and theft of confidential data. One government institution that is making the most of IT's benefits is the police institution [5]. The motorized vehicle administration service unit in the police is one of the public service units that make maximum use of IT to provide community services.

The police institution in the Banyumas area, Central Java, collaborates with civilian government institutions to try to make maximum use of the IT function in administrative services to operate the motorized vehicle testing system. The service system is called Vehicle Testing of Management Information System (VTMIS). VTMIS is an integrated motorized vehicle system owned by the police institution that functions for administrative management related to the motor vehicle testing process, starting from the registration process, paying levies, and testing vehicles in the Banyumas transportation service area. Because the police service unit is so essential, it is necessary to have IT management, supervision, and maintenance in this police unit. However, the maximum use of IT by VTMIS needs to pay attention to risk management which must run simultaneously when the system is also operating.

Regarding risks or threats that occur in operations, the police, through VTMIS hopes to get input, in this case, a solution to reduce the level of the risk, to overcome risks that often occur and risks that rarely happen in the company. Therefore, the police need Information Technology

Governance (ITG) to mitigate and reduce the risk that has already occurred [6]. With ITG based on risk analysis, the police institution will have strong IT governance and support their business strategy [7]. From the explanation of the research background, two research questions guide the implementation of the research.
RQ1: What is the risk management maturity level in terms of the Plan and Organize Domain in VTMIS?
RQ2: What recommendations are given based on the risk management maturity level in VTMIS?

II. Literature Review

Control Objective for Information and Related Technology (COBIT) 4.1 is a medium for measuring IT governance. Use of COBIT 4.1 for VTMIS risk management analysis of police institutions, especially the Plan and Organize (PO) domain [8], [9]. IT governance aligns IT investment with business strategy and eliminates the risks of using IT [10]. IT governance is part of corporate governance that focuses on IT management in organizations, including IT system performance and risk management [11]. COBIT 4.1 is useful for managers, audiences, and IT users in the form of a procedural sequence of action steps to maximize the benefits of using IT [12]. COBIT 4.1 mission is to conduct research, development, publishing, promotion of papers, updating the sequence or provisions of an IT Control Purpose. Meanwhile, the vision of COBIT 4.1 is to make CO-BIT a model for IT control and management [13]. The following are the 4 Domains of the COBIT 4.1 variable:
1. Plan and Organize (PO)
2. Acquire and Implementation (AI)
3. Deliver and Support (DS)
4. Monitoring and Evaluation (ME).

1. *Plan and Organize (PO)*

This domain contains strategies and IT identification tactics that can best contribute to achieving the organization's business goals to become a good organization with the right technology infrastructure. The domain has 11 indicators as in table I:

TABEL I
Indicator Of Plan And Organize

Indicator	Describe
PO1	Determine a strategic information technology plan.
PO2	Define the information architecture.
PO3	Specify technology direction.
PO4	Define IT organization and relationships.
PO5	Manage investment in information technology
PO6	Communicate management objectives and direction.
PO7	Manage human resources.
PO8	Manage quality
PO9	Assess risk.
PO10	Manage the project.

2. *Acquire and Implement (AI)*

This domain contains IT strategy realization, identification of IT solutions, building IT, and integration of IT into business processes. This domain has 7 indicators, as in table II:

TABEL II
Indicator Of Acquire And Implementation

Indicator	Describe
AI1	Identifies automatic solutions
AI2	Acquire and maintain application software
AI3	Acquire and maintain technology infrastructure
AI4	Develop and maintain IT procedures
AI5	Meets IT Data Sources
AI6	Managing change
AI7	Installing and accrediting systems and their changes

3. *Delivery and Support (DS)*

This domain serves to provide security process services, business continuity aspects, and provision of training. The domain has 13 indicators, as in table III:

TABEL III
Indicator Of Delivery And Support

Indicator	Describe
DS1	defines and manages service levels
DS2	manages third party services
DS3	manages performance and capacity
DS4	ensures continuous service
DS5	ensures system safety
DS6	identifies and allocates costs
DS7	educates and trains users
DS8	manages service and incidents
DS9	manages configuration
DS10	manages problems
DS11	manages data
DS12	manages Facilities
DS13	manages operations

4. *Monitor and Evaluation (ME)*

This domain functions to periodically assess IT processes based on the quality and suitability of control requirements. The domain has 4 indicators, as in table IV:

TABEL IV
Indicator Of Monitor And Evaluation

Indicator	Describe
ME1	supervises and evaluates IT performance
ME2	supervises and evaluates internal controls
ME3	ensures fulfillment of external needs
ME4	provides IT governance

Based on the description of the four COBIT 4.1 domains, the PO9 domain serves as the main tool for describing risk management assessments in the Banyumas Police VTMIS application. Figure of the overall COBIT 4.1 Framework as in Figure 1:

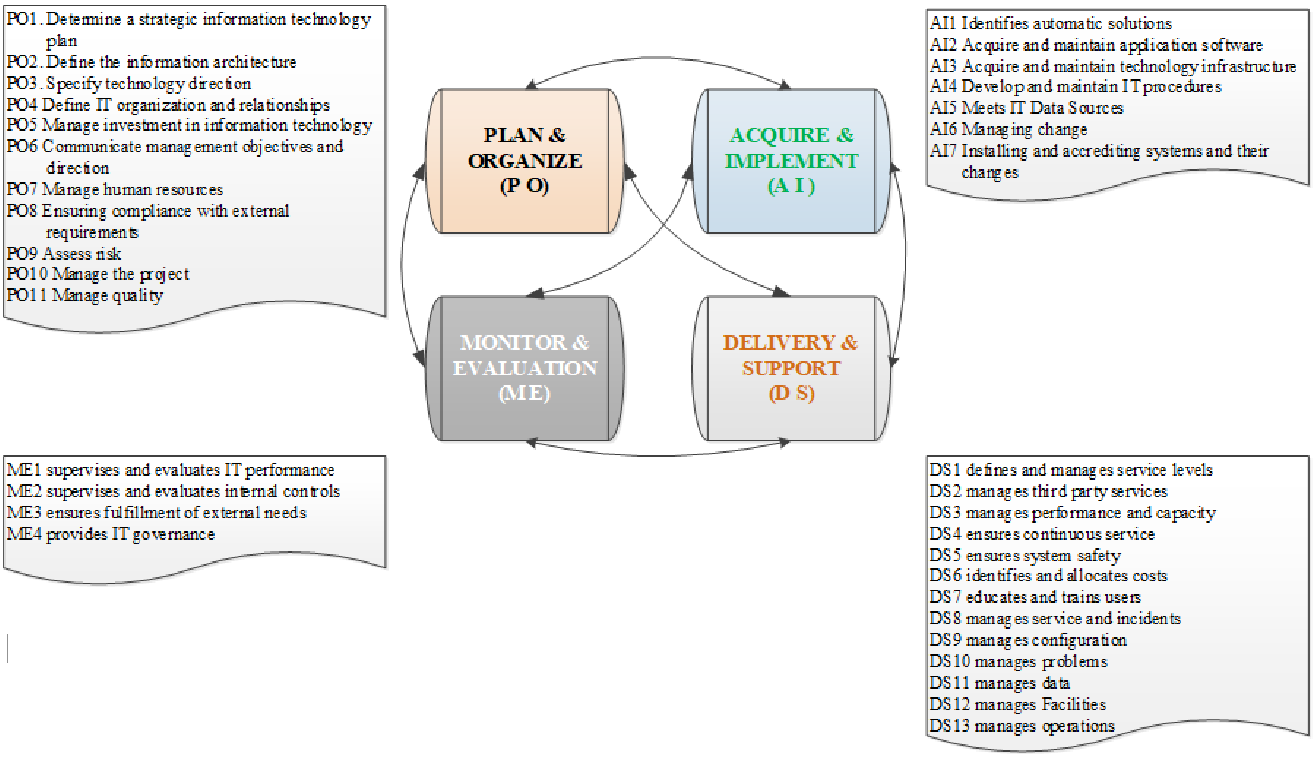
PO1. Determine a strategic information technology plan
PO2. Define the information architecture
PO3. Specify technology direction
PO4 Define IT organization and relationships
PO5 Manage investment in information technology
PO6 Communicate management objectives and direction
PO7 Manage human resources
PO8 Ensuring compliance with external requirements
PO9 Assess risk
PO10 Manage the project
PO11 Manage quality
PLAN & ORGANIZE (P O)
ACQUIRE & IMPLEMENT (A I)
AI1 Identifies automatic solutions
AI2 Acquire and maintain application software
AI3 Acquire and maintain technology infrastructure
AI4 Develop and maintain IT procedures
AI5 Meets IT Data Sources
AI6 Managing change
AI7 Installing and accrediting systems and their changes
MONITOR & EVALUATION (ME)
DELIVERY & SUPPORT (D S)
ME1 supervises and evaluates IT performance
ME2 supervises and evaluates internal controls
ME3 ensures fulfillment of external needs
ME4 provides IT governance
DS1 defines and manages service levels
DS2 manages third party services
DS3 manages performance and capacity
DS4 ensures continuous service
DS5 ensures system safety
DS6 identifies and allocates costs
DS7 educates and trains users
DS8 manages service and incidents
DS9 manages configuration
DS10 manages problems
DS11 manages data
DS12 manages Facilities
DS13 manages operations

Figure 1. COBIT 4.1 Framework

A. *Maturity Level of COBIT 4.1*

COBIT 4.1 has a maturity level to control IT processes using the assessment method to assess their IT processes on a scale from 0 to 5. The maturity level of COBIT 4.1 in table V:

TABEL V
MATURITY LEVEL OF COBIT 4.1

Value	Describe
0 – 0.5	0: Not Existent
0.51– 1.50	1: Initial
1.51-2.50	2: Repeatable but Intuitive
2.51-3.50	3: Defined Process
3.51-4.50	4: Managed and Measurable
4.51-5.00	5: Optimized

B. *Compliance Value*

The measurement technique in the maturity level uses several questions, and each question has a group of appropriateness using a standard assessment as shown in table VI:

TABEL VI
COMPLIANCE VALUE

Scale	Statement of Compliance Value	Compliance Value
1	Not true	0
2	Little truth	0.33
3	Most of it is true	0.66
4	Correct	1

The research method process takes steps starting from the research procedure, determining and taking data samples, data analysis, discussion, and concluding. The analysis conducted is descriptive and inferential maturity level analysis, limitations, and research recommendations supported by other studies.

III. METHOD

Figure 2 describe the research procedures:

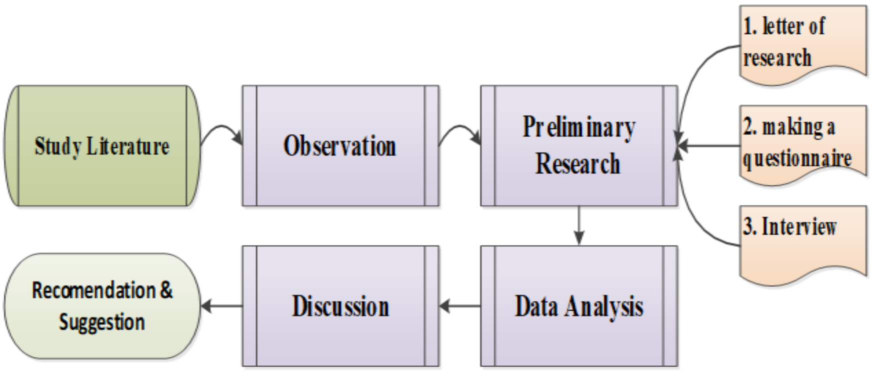

Figure 2. The Research Procedure

A. Study Literature

It requires an understanding of the maturity level of risk management for the COBIT 4.1 at P09 domain as a reference for assessing digital bus transportation services.

B. Observation

It made initial observations by conducting a questionnaire instrument test and interviewing several VTMIS staff members before distributed the revised questionnaire.

C. Preliminary Research

It is conducted by obtaining research approval for the research object, making revisions to the questionnaire, becoming the primary research questionnaire, and conducting interviews with several new respondents. The Instrument test is determining the validity and reliability of the questionnaire questions.

For the validity test, the product-moment correlation technique to test validity. The validity test is useful for knowing whether the measuring instrument measures what needs to be measured. Product is implementing method by correlating each question with the total score for each variable. Correlation figures obtained statistically must be compared with the critical statistics of the correlation table of r values with a significant level of 95%. r count> r table means that the data is substantial (valid) and suitable for hypothesis testing. And vice versa if r count <from r table indicates, the information data is not significant (invalid) and will not be included in testing the research hypothesis.

$$r_{count}=\frac{n(\sum XY)-(\sum X)(\sum Y)}{\sqrt{(n\sum X^2)-(\sum X)^2(n\sum y^2-(\sum Y)^2)}}$$
(2)

r_{count}: correlation coefficient between X and Y variables
N: number of respondents
Σ_X: total scores of the items
Σ_Y: total scores of questions
$\Sigma_X{}^2$: total score squares of the items
$\Sigma_Y{}^2$: total score of the squares of the items

The reliability test determines whether the data collection tool showed accuracy, stability, or consistency in expressing individuals specific symptoms, even though it did at different times. Reliability test is on statements that are already valid. This test uses the Cronbach alpha technique because the answer value consists of a range of deals with the larger alpha coefficient. Reliability means trustworthy "That is, the instrument can give the right results.

$$r_{instrument} = \left(\frac{n}{n-1}\right)\left(1-\frac{\sum {s_i}^2}{\sum {s_t}^2}\right) \qquad (3)$$

$r_{\text{instrument}}$: reliability of instrument
n: number of questions
s_i^2: variance of item
s_t^2: total variance

D. Data Analysis

It analyzes the data using COBIT 4.1 specifically for the domain in P09 to determine the maturity level of risk management.

It needs to normalize value data to calculate the maturity level of the P09 domain. The process is normalizing value from each group by dividing each compliance value by the total compliance value. The second step gets each level contribution value by multiplying the respective compliance values to the individual level values. The calculation of contribution value is the maturity level index.

$$\mathrm{NV} = \frac{\mathrm{CV}}{\mathrm{TCV}} \tag{4}$$

NV: Normalize data Value
CV: Compliance Value
TCV: Total Compliance Value

$$\mathrm{CONV} = \frac{\mathrm{CV}}{\mathrm{LV}} \tag{5}$$

CONV: Contribution Value
CV: Compliance Value
LV: Level

$$\mathrm{ML} = \sum \mathrm{CONV} \tag{6}$$

ML: Maturity Level
CONV: Contribution Value

E. *Discussion*

It needs to clarify by comparing the results of research data analysis by conducting discussions by comparing them with previous research by experts regarding risk management and VTMIS applications.

F. *Recommendation and Suggestion*

It concludes the discussion results and makes positive recommendations for VTMIS. It also provides suggestions for ongoing research for other researchers who are interested in continuing this research.

IV. Result and Discussion

The first step in data analysis is to identify the respondent profile. In table VII, questionnaire respondents in the VTMIS environment have various education levels, work types, computer skills.

TABEL VII
THE RESPONDENT PROFILE

Standard	Indicator	%
Job position	Management of VTMIS staff of VTMIS	22 78
Education level	Magister Bachelor Associate degree	22 50 28
Computer Skill	Good Enough Less	12 50 38

A. *Validity Test*

The data obtained and inputted into the validity formula for the validity test instrument results, as shown in Table VIII;

TABEL VIII
VALIDITY TEST P09 (LEVEL 0-5)

Level	N of Items	Average r_{count}	r_{table}	result
0	3	0.870	0.561	Valid
1	7	0.880	0.573	Valid
2	3	0.871	0.561	Valid
3	6	0.879	0.570	Valid
4	11	0.902	0.585	Valid
5	7	0.883	0.573	Valid

B. *Reliability Test*

The results of the reliability test were coming from the research data. It input into the reliability formula as in Table IX:

TABEL IX
RELIABILITY TEST P09 (LEVEL 0-5)

Cronbach Alpha	Cronbach Alpha based on standardized items	N of items
.946	.932	3
.961	.951	7
.945	.941	3
.946	.942	6
.963	.960	11
.947	.945	7

C. *Maturity Level Test*

The maturity level test results of risk management at VTMIS using the COBIT 4.1 domain of P09 (Assess risk) as in Table X; Table XI; Table XII; Table XIII; Table XIV; Table XV.

TABEL X
COMPLIANCE LEVEL 0

Maturity Level 0		0	0.33	0.66	1	
No	Statement					
1	risk assessment does not occur.	3	1	2	12	13.05
2	the organization does not consider security vulnerabilities	6	1	2	9	10.65
3	risk management is not relevant to acquiring IT solutions	3	1	2	12	13.65
	Total					37.95
	Compliance Value					12.65

TABEL XI
COMPLIANCE LEVEL 1

Maturity Level 1		0	0.33	0.66	1	
No	Statement					
1	an ad hoc manner that	8	5	2	3	5.97

Maturity Level 1		0	0.33	0.66	1	
No	**Statement**					
	considered IT risks					
2	each project determines assessments of project risk	9	4	2	3	5.64
3	risk assessments are rarely implemented to specific managers.	4	7	2	5	8.63
4	a project uses risk assessment occasionally	3	2	4	9	12.3
5	management meetings seldom discuss risk assessment	11	3	1	3	4.65
6	where risks have been considered, mitigation is inconsistent.	6	3	2	7	9.31
7	It is are essential to understand IT risks		4	1	13	14.98
	Total					61.48
	Compliance Value					8.78

TABEL XII
COMPLIANCE LEVEL 2

Maturity Level 2		0	0.33	0.66	1	
No	**Statement**					
1	there is a risk assessment by project managers	2	2	2	12	13.98
2	only to significant projects or response to problems applies the RA	3	2		13	13.66
3	If there is a risk only then starting mitigation processes	4	1	1	12	12.99
	Total					40.63
	Compliance Value					13.54

TABEL XIII
COMPLIANCE LEVEL 3

Maturity Level 3		0	0.33	0.66	1	
No	**Statement**					
1	there is an organization-wide risk management policy.	2	2	1	13	14.32
2	there is risk management training is available to all staff members.	14	2		2	2.66
3	every individual has their own decisions to follow the risk management process and receive training.	15	2	1		1.32
4	the risk assessment ensures that key risks to the business are identified.	11	1	1	5	5.99
5	once the risks are identified, then a process to mitigate key risks is on.	15	2	1		1.32
6	there is a job description that considers risk management responsibilities.	4	4	2	8	10.64
	Total					36.25
	Compliance Value					6.04

TABEL XIV
COMPLIANCE LEVEL 4

Maturity Level 4		0	0.33	0.66	1	
No	**Statement**					
1	the assessment and management of risk are standard procedures		2	1	15	16.32
2	IT management needs the risk management process reporting.		6	1	11	13.64

Maturity Level 4		0	0.33	0.66	1	
No	**Statement**					
3	IT risk management is a senior management-level responsibility.	3	2	1	12	13.32
4	risk is assessed and mitigated at the individual project level.	1	4	7	6	11.94
5	Management receives advice on changes in the business and IT environment that could significantly affect the IT-related risk scenarios.	9	3	2	4	6.31
6	Management monitors the risk position	3	5	2	8	10.97
7	Top management (senior and IT unit) establish the firm RA will put up with all identified risks have a nominated.		1	2	15	16.65
8	developing the normal management based on RA and RD	1	2	1	14	15.32
9	there is a management budget for an operational risk		6	3	9	12.96
10	there is a risk assessment, and management processes are starting to be operated	2	1	4	11	13.97
11	IT management considers risk mitigation strategies.	1	4	4	9	12.96
	Total					144.36
	Compliance Value					13.12

TABEL XV
COMPLIANCE LEVEL 5

Maturity Level 5		0	0.33	0.66	1	
No	**Statement**					
1	risk management develops to the stage organization well managed	3	5	4	6	10.29
2	acceptable risk management practices across the entire organization.	8	6	1	3	5.64
3	reporting of risk management data is highly automated.	7	3	2	6	8.31
4	risk assessment criteria based on firm top management in the field	3	4	2	9	11.64
5	risk assessment merges business and IT system	3	4	2	9	11.31
6	Management detects and acts without consideration of the risk management plan.	9	4	2	3	5.64
7	Management continues to assess risk mitigation strategies.	3	1	1	13	13.99
	Total					66.82
	Compliance Level					9.55

TABEL XVI
MATURITY LEVEL OF ASSESS RISK

PO9 maturity level calculation (level 0-5)			
Level	**Compliance**	**Normalize**	**Contribution**
0	12.65	0.1986495	0
1	8.78	0.1378769	0.137876884
2	13.54	0.2126256	0.425251256
3	6.04	0.0948492	0.284547739
4	13.12	0.2060302	0.824120603
5	9.55	0.1499686	0.749842965
	63.68	ML	2.421639447

D. *Discussion*

This research uses quantitative study analysis in literature review. Quantitative study analysis helps analyse through data processing approaches using statistical or mathematical methods [14], and the use of quantitative techniques also needs to pay attention to ethics in research analysis so that ethical quality is also maintained [15]. The respondent profile aims to describe the strength of research data that is trusted, accurate, and accountable [16]. Based on the reliability test, it shows if the questionnaire has a consistent quality of questions so that it can become a questionnaire as a measuring tool.

This research requires mapping to the COBIT 4.1 domain to describe the communication and control relationships in an IS development project [17]. One of the Domains in COBIT 4.1, namely the P09 Domains, helps analyse risk management [18]. Based on the maturity level test in risk management, it implies that the risk assessment process is still in the procedural stage. The resulting recommendation for VTMIS is the need for special training related to IT risk management in each process unit to provide an overview of how to mitigate IT risks.

Service becomes the first motto along with the development of information systems through service applications significantly affecting application development companies [13], [19]. The possibility of application errors in the system is very high related to risks in TI. A researcher said if the study of risk assessment methods to identify the presence of IT system sustainability aspects through the COBIT framework [20]. COBIT presents a detailed analysis of how organizations use this model [21]. This research through COBIT tries to check and analysis IT and firm risk to a good governance. This article also analyses the information based on the business and the scope of future research.

V. Conclusion

The maturity level of VTMIS risk management is 2.42. The position level is at level 2, Repeatable but intuitive, meaning that the risk assessment process is still in the procedure stage. There is no specific training related to IT risks, and the possibility of application errors in the system is high risk in IT. The resulting recommendation for VTMIS is there needs to be special training related to IT risk management in each process unit to provide an overview of how to mitigate IT risks. Suggestions for further research with the object of IT risk management is to add monitor and evaluation domains as additional domains when researching so that monitoring and analysis can be more accurate.

Daftar Pustaka

[1] A. K. Tawalbeh and M. A. Niqresh, “The Role of Specialists in Improving the Quality of Government Institutions ’ Information Documentation During COVID 19,” *Int. J. Contemp. Manag. Inf. Technol.*, vol. 1, no. 2, pp. 7–15, 2021.

[2] C. Chen, J. Ma, Y. Susilo, Y. Liu, and M. Wang, “The promises of big data and small data for travel behavior (aka human mobility) analysis,” *Transp. Res. Part C Emerg. Technol.*, vol. 68, pp. 285–299, 2016, doi: 10.1016/j.trc.2016.04.005.

[3] N. Poritskiy, F. Oliveira, and F. Almeida, “The benefits and challenges of general data protection regulation for the information technology sector,” *Digit. Policy, Regul. Gov.* , vol. 21, no. 5, pp. 510–524, 2019, doi: 10.1108/DPRG-05-2019-0039.

[4] N. BATYASHE and T. IYAMU, “Operationalisation of the Information Technology strategy in an organisation,” *J. Contemp. Manag.*, vol. 17, no. 2, pp. 198–224, 2020, doi: 10.35683/jcm20018.71.

[5] L. Garicano and P. Heaton, “Information technology, organization, and productivity in the public sector: Evidence from police departments,” *J. Labor Econ.*, vol. 28, no. 1, pp. 167–201, 2010, doi: 10.1086/649844.

[6] M. Benaroch and A. Chernobai, “OPERATIONAL IT FAILURES, IT VALUE DESTRUCTION, AND BOARD-LEVEL IT GOVERNANCE CHANGES,” *MIS Q.*, vol. 41, no. 3, pp. 729–742, 2017, doi: 10.3109/10731199409117662.

[7] P. Durán Santomil and L. Otero González, “Enterprise risk management and Solvency II: the system of governance and the Own Risk and Solvency Assessment,” *J. Risk Financ.*, vol. 21, no. 4, pp. 317–332, 2020, doi: 10.1108/JRF-09-2019-0183.

[8] M. S. De Araujo, E. C. Oliveira, S. B. S. Monteiro, and T. M. F. De Queiroz Mendonça, “Risk management maturity evaluation artifact to enhance enterprise IT quality,” *ICEIS 2017 - Proc. 19th Int. Conf. Enterp. Inf. Syst.*, vol. 3, no. Iceis, pp. 425–432, 2017, doi: 10.5220/0006324404250432.

[9] F. M. Alkhaldi, S. M. Hammami, and M. A. Uddin, “Understating value characteristics toward a robust IT governance application in private organizations using COBIT framework,” *Int. J. Eng. Bus. Manag.*, vol. 9, pp. 1–8, 2017, doi: 10.1177/1847979017703779.

[10] G. L. Lunardi, A. C. G. Maçada, J. L. Becker, and W. Van Grembergen, “Antecedents of IT governance effectiveness: An empirical examination in Brazilian firms,” *J. Inf. Syst.*, vol. 31, no. 1, pp. 41–57, 2017, doi: 10.2308/isys-51626.

[11] M. El Khatib, L. Nakand, S. Almarzooqi, and A. Almarzooqi, “E-Governance in Project Management: Impact and Risks of Implementation,” *Am. J. Ind. Bus. Manag.*, vol. 10, no. 12, pp. 1785–1811, 2020, doi: 10.4236/ajibm.2020.1012111.

[12] D. Haouam, “IT governance impact on financial reporting quality using COBIT framework,” *Glob. J. Comput. Sci. Theory Res.*, vol. 10, no. 1, pp. 1–10, 2020, doi: 10.18844/gjcs.v10i1.4143.

[13] J. Aguiar, R. Pereira, J. B. Vasconcelos, and I. Bianchi, “An overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC),” *Interdiscip. J. Information, Knowledge, Manag.*, vol. 13, pp. 137–163, 2018, doi: 10.28945/4083.

[14] M. S. Rahman, “The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language ‘Testing and Assessment’ Research: A Literature Review,” *J. Educ. Learn.*, vol. 6, no. 1, p. 102, 2016, doi: 10.5539/jel.v6n1p102.

[15] M. J. Zyphur and D. C. Pierides, “Is Quantitative Research Ethical? Tools for Ethically Practicing, Evaluating, and Using Quantitative Research,” *J. Bus. Ethics*, vol. 143, no. 1, pp. 1–16, 2017, doi: 10.1007/s10551-017-3549-8.

[16] A. Sturrock, A. Marsden, C. Adams, and J. Freed, “Observational and Reported Measures of Language and Pragmatics in Young People with Autism: A Comparison of Respondent Data and Gender Profiles,” *J. Autism Dev. Disord.*, vol. 50, no. 3, pp. 812–830, 2020, doi: 10.1007/s10803-019-04288-3.

[17] S. Gantman and J. Fedorowicz, “Communication and control in outsourced IS development projects: Mapping to COBIT domains,” *Int. J. Account. Inf. Syst.*, vol. 21, pp. 63–83, 2016, doi: 10.1016/j.accinf.2016.05.001.

[18] J. F. Andry, G. Wang, G. N. Suryantara, and D. Y. Bernanda, “Assessing The COBIT Maturity Model in Manufacturing Company,” *Int. J. New Media Technol.*, vol. 5, no. 2, pp. 109–115, 2019, doi: 10.31937/ijnmt.v5i2.927.

[19] M. Jäntti and A. Cater-Steel, "Proactive Management of IT Operations to Improve IT Services," *J. Inf. Syst. Technol. Manag.*, vol. 14, no. 2, pp. 191–218, 2017, doi: 10.4301/s1807-17752017000200004.

[20] P. Mulgund, P. Pahwa, and G. Chaudhari, "Strengthening IT Governance and Controls Using COBIT," *Int. J. Risk Conting. Manag.*, vol. 8, no. 4, pp. 66–90, 2019, doi: 10.4018/ijrcm.2019100104.

[21] 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.