FINAL PROJECT

DESIGNING INFORMATION TECHNOLOGY GOVERNANCE FOR DIGITAL TRANSFORMATION IN XYZ PROVINCIAL GOVERNMENT USING COBIT 2019 FRAMEWORK

Supervisor 1: Ryan Adhitya Nugraha, S.T., M.T., CISA.
Supervisor 2: Dr. Yuli Adam Prasetyo, S.T.,M.T.

Examiner 1: Iqbal Yulizar Mukti, S.Si, M.T., Ph.D
Examiner 2: Falahah, S.Si., M.T.

FACULTY OF INDUSTRIAL ENGINEERING
INFORMATION SYSTEM
TELKOM UNIVERSITY

2025

OUR TEAM

Gaitsa Zahira Shafa
(1202210379)

Dita Amalia Putri
(1202210409)

Sarnia Humaira Thamrin
(1202213204)

CHAPTER I
INTRODUCTION

BACKGROUND

- The rapid development of digital transformation in Indonesia
- XYZ Provincial Government actively participates in digital transformation initiatives
- Many digital transformation initiatives fail due to weak IT governance
- XYZ Provincial Government has never conducted a formal COBIT 2019-based assessment for IT governance and management
- A structured and appropriate IT governance design is needed to support digital transformation in XYZ Provincial Government

PROBLEM STATEMENT

1. What is the existing condition of IT governance in XYZ Provincial Government?
2. How is the gap analysis between the existing condition of IT governance in XYZ Provincial Government and the standards set in the COBIT 2019 framework?
3. How is the IT governance design for digital transformation in XYZ Provincial Government using the COBIT 2019 framework?
4. What is the level of IT governance capability in XYZ Provincial government if the draft recommendations are implemented?

OBJECTIVE

1. Analyze and understand the existing conditions of IT governance in XYZ Provincial Government.
2. Analyzing the gap between existing conditions and IT governance standards based on the COBIT 2019 framework.
3. Designing IT governance to support digital transformation in XYZ Provincial Government using the COBIT 2019 framework.
4. Evaluate the level of capability of IT governance in XYZ Provincial Government if the draft recommendations are implemented.

SCOPE

The IT governance design in this research is focused on the Align, Plan, and Organize (APO), Build, Acquire, and Implement (BAI), Evaluate, Direct, and Monitor (EDM), and Monitor, Evaluate, and Assess (MEA) domains based on the COBIT 2019 framework.

BENEFITS

- For XYZ Provincial Government: As a reference to increase the effectiveness of IT governance and support the optimization of digital transformation.
- For Researchers: As a means of developing skills in designing IT governance based on COBIT 2019.
- For Other Researchers: As a reference in research related to the implementation of IT governance in the government sector or related organizations.

CHAPTER II
LITERATURE REVIEW

THEORETICAL FOUNDATION

INFORMATION TECHNOLOGY

Information Technology (IT) refers to the tools used to manage and process data into accurate and relevant information that supports decision-making, enhances operational efficiency, and serves as the foundation for modern public services

INFORMATION TECHNOLOGY GOVERNANCE

IT Governance involves the structures and processes that ensure IT usage aligns with organizational goals, creates value, and minimizes risk by integrating people, processes, and technology in a coordinated manner.

DIGITAL TRANSFORMATION

Digital transformation is a strategic process of leveraging digital technologies to improve services, organizational efficiency, and value creation, particularly in facing technological disruption and growing public demands.

COBIT FRAMEWORK 2019

COBIT 2019 is a globally recognized framework by ISACA for governing and managing enterprise IT. It provides 40 Governance and Management Objectives (GMOs) across 5 domains, emphasizing a goal-oriented approach and customizable design to suit different organizational contexts

PREVIOUS RESEARCH

a.

DARMAWAN & WIJAYA (2022)

Implementation of COBIT 2019 for designing an integrated IT governance system aligned with business strategy

b.

Abror et al. (2024)

IT governance audit in BMKG with COBIT 2019 revealed several areas below target maturity levels, with improvement plans suggested

c.

Rizaldi et al. (2024)

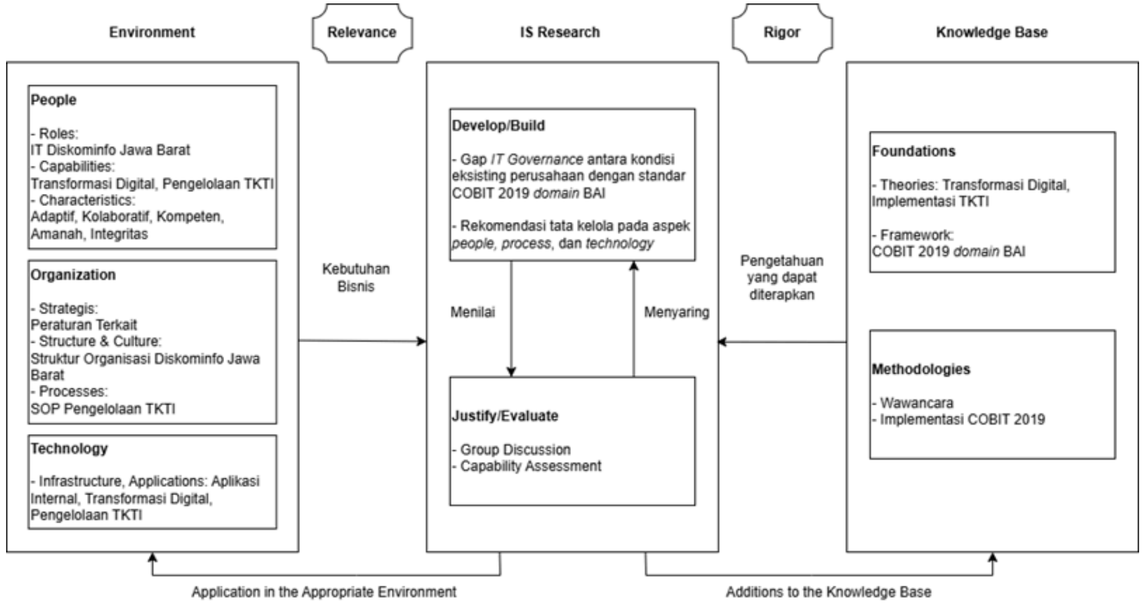
Ambidextrous governance using COBIT proved to improve governance capability and support digital transformation in UMKM BPRACo

BAB III
RESEARCH METHODOLOGY

FRAME OF MIND

Adopting Design Science Research (DSR) as a conceptual framework.

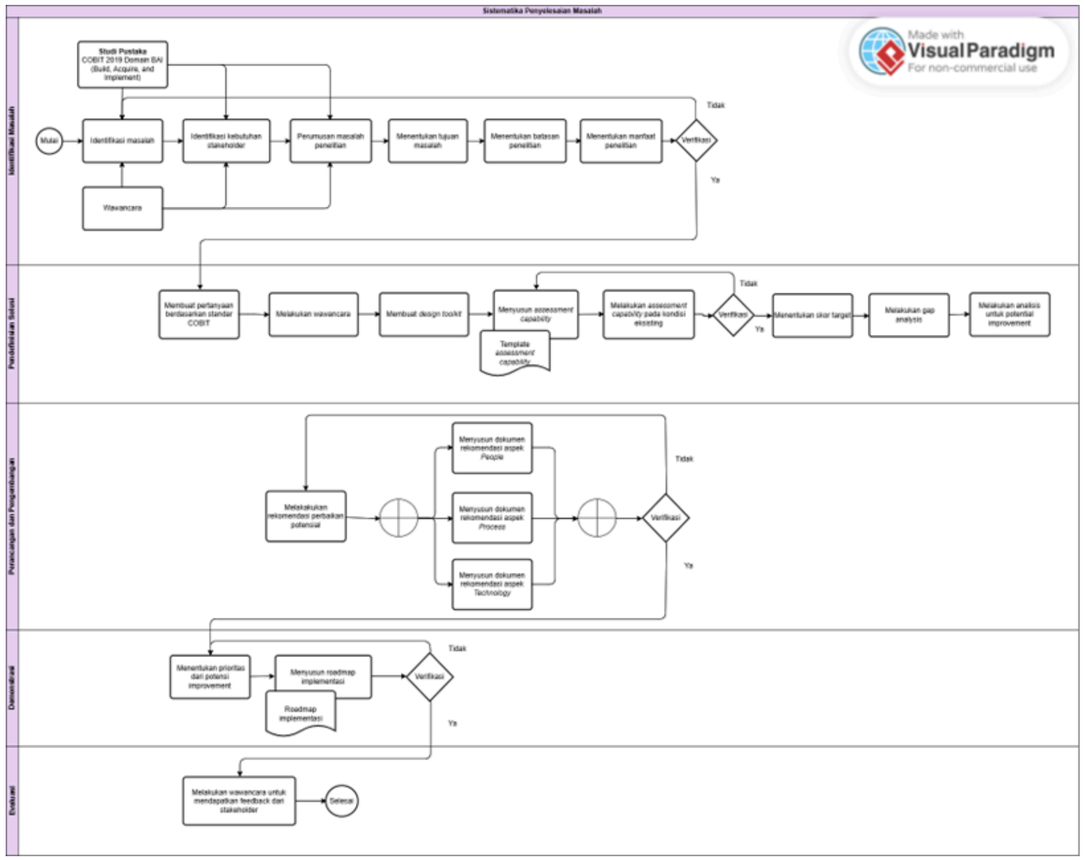
- The environment serves as a research support tool to help design the management information design and governance roadmap.
- IS Research, which includes two main aspects, namely development/build and justify/evaluate.
- The knowledge base in this research will be used as a reference in the research. The scope of the knowledge base is divided into two main parts, namely foundations and methodologies.



PROBLEM SOLVING SYSTEMATICS

This research follows the five main stages in design science research:

1) first phase "Problem identification and motivation"
2) second phase "Define goals for the solution"
3) third phase "Design and development"
4) fourth phase "Demonstration"
5) fifth phase "Evaluation"



DATA COLLECTION

Data collection was carried out through two main methods, namely primary data and secondary data.

Primary Data

Data Source	Method Objective	Collection
Relevant stakeholders in XYZ Provincial	Interviews by interacting directly with relevant stakeholders	Identifying domain gaps with COBIT 2019 standards

Secondary Data

Data Source	Method Objectives	Collection
Internal documents such as SOPs, organizational structures, and performance reports	Using document triangulation by reviewing relevant internal documents	Support validation of primary data

DATA PROCESSING

Data analysis is carried out qualitatively on the results obtained during the assessment process. Preparation of an assessment to identify the existing condition of IT governance in the XYZ Provincial Government, with reference to the 2019 COBIT framework for each domain.

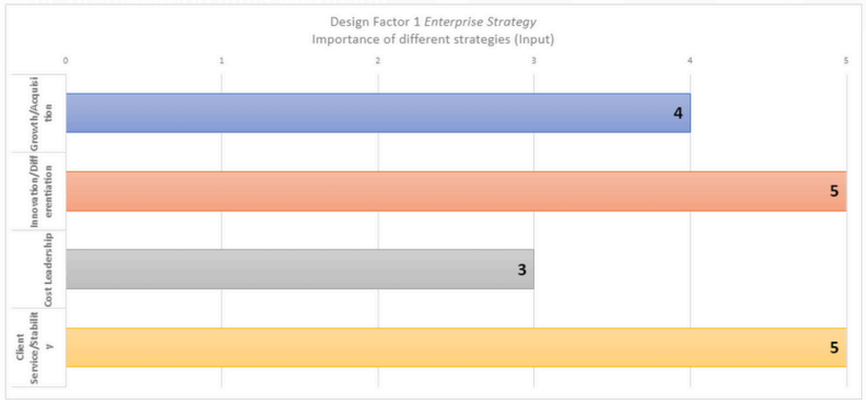
EVALUATION METHOD

The evaluation method in this study was conducted using a stakeholder feedback-based approach. This verification aims to ensure that the draft recommendations generated from the analysis are in accordance with the conditions of the organization. The feedback provided by the stakeholders became the basis for revising and refining the research results.

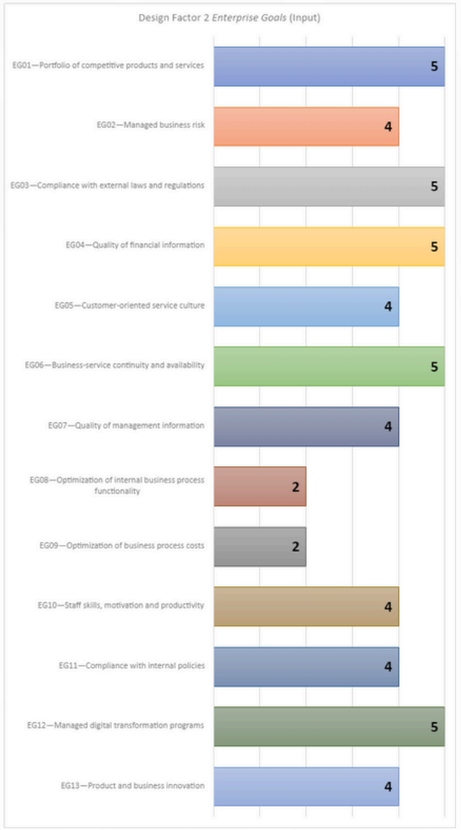
CHAPTER IV
DATA COLLECTION AND DATA ANALYSIS

ANALYSIS OF COBIT 2019 DESIGN FACTORS (DF)

DF1:Enterprise Strategy

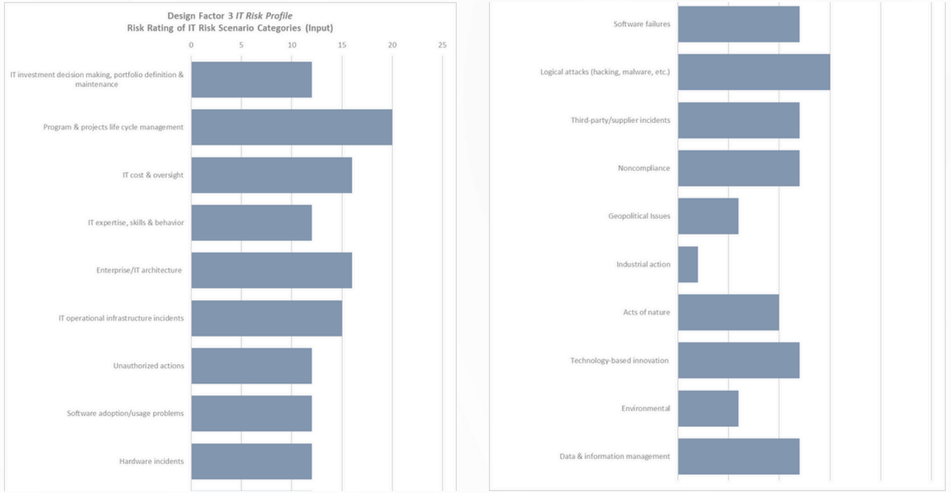


DF2: Enterprise Goals

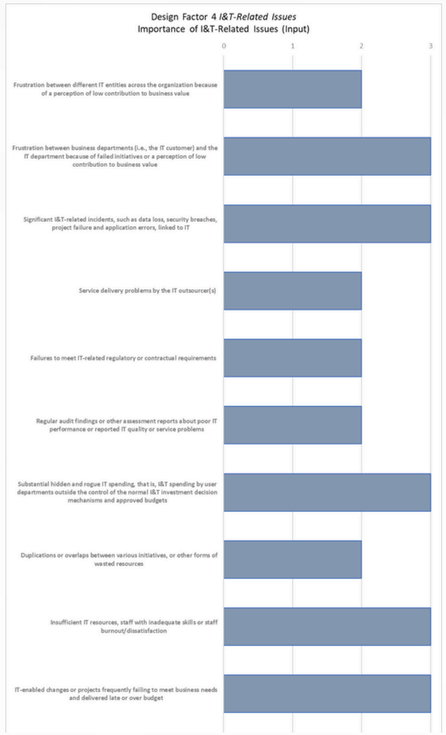


ANALYSIS OF COBIT 2019 DESIGN FACTORS (DF)

DF3:Risk Profile

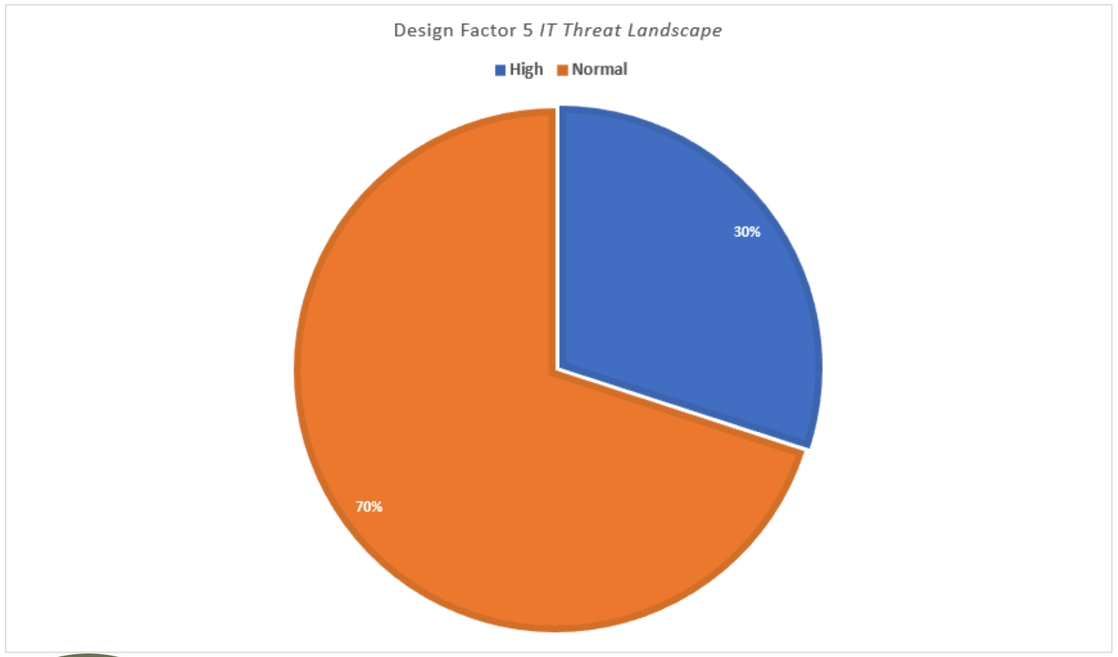


DF4: I&T Related-Issues

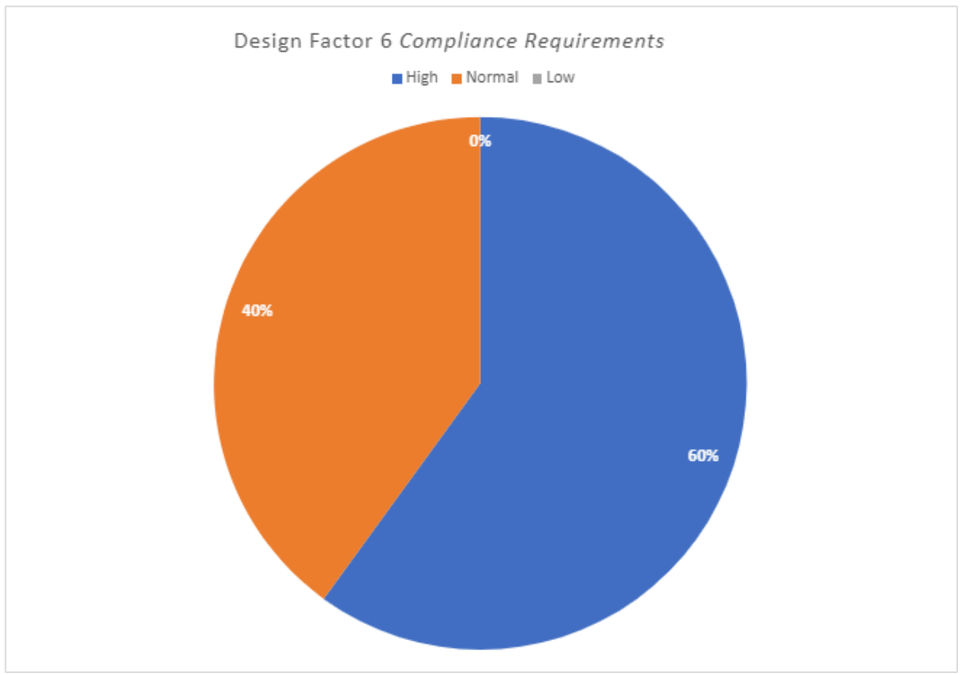


ANALYSIS OF COBIT 2019 DESIGN FACTORS (DF)

DF5: Threat Landscape

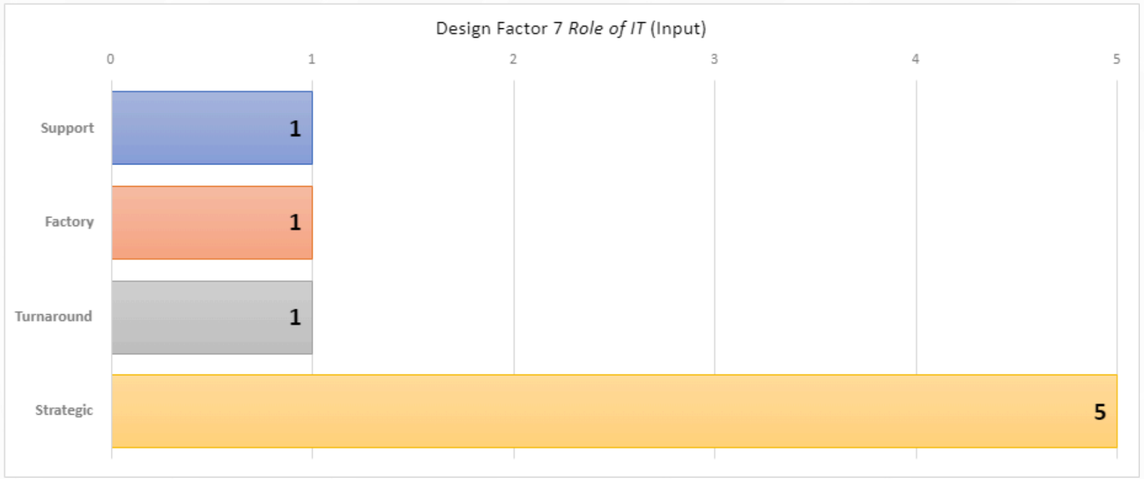


DF6: Compliance Requirements

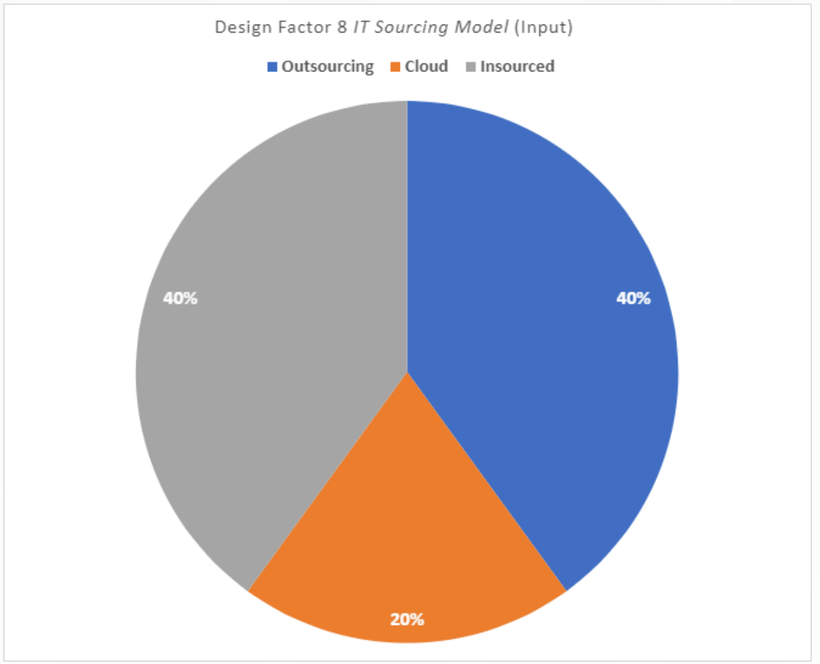


ANALYSIS OF COBIT 2019 DESIGN FACTORS (DF)

DF7: Role of IT

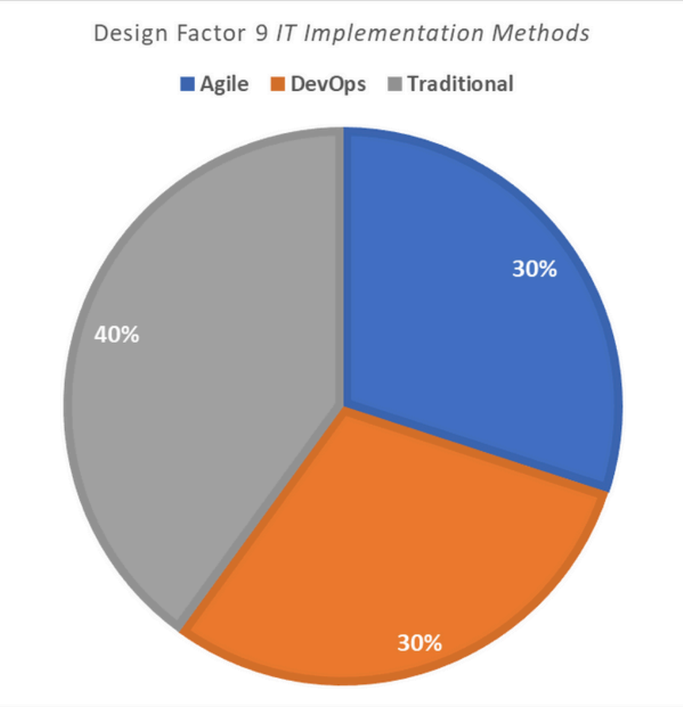


DF8: IT Sourcing Model

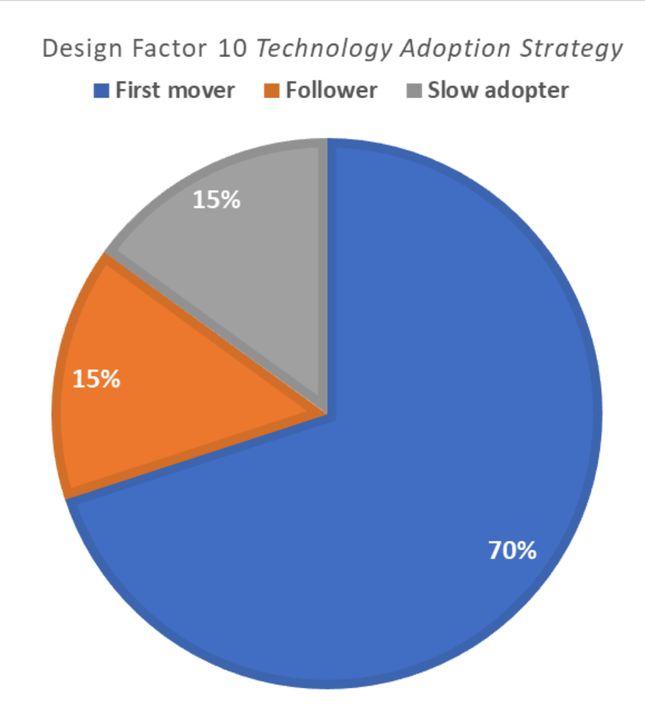


ANALYSIS OF COBIT 2019 DESIGN FACTORS (DF)

DF9: IT Implementation Methods



DF10: Technology Adoption Strategy



DOMAIN EDM & MEA

Presentation by Sarnia Humaira Thamrin

RESULTS OF DESIGN FACTOR & CAPABILITY ASSESSMENT IN EDM AND MEA DOMAINS

EDM & MEA domain prioritization results

No	No	No
1	EDM03—*Ensured Risk Optimization*	75
2	MEA03—*Managed Compliance with External Requirements*	75
3	EDM01—*Ensured Governance Framework Setting & Maintenance*	50
4	MEA04—*Managed Assurance*	50

Capability Assessment EDM01

EDM01—*Ensured Governance Framework Setting & Maintenance*				
No	**Governance Practice**	**Achievement**	**Capability Level**	**Target**
1	EDM01.01 *Evaluate the governance*	100% F (*Fully*)	2	3
		100% F (*Fully*)	3	
2	EDM01.02 *Direct the governance system.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
3	EDM01.03 *Monitor the governance system.*	100% F (*Fully*)	3	

Capability Assessment EDM03

EDM03—*Ensured Risk Optimization*				
No	**Governance Practice**	**Achivement**	**Capability Level**	**Target**
1	EDM03.01 *Evaluate risk management*	100% F (*Fully*)	2	4
		100% F (*Fully*)	3	
2	EDM03.02 *Direct risk management.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
3	EDM03.03 *Monitor risk management.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
		100% F (*Fully*)	4	

RESULTS OF CAPABILITY ASSESSMENT IN EDM AND MEA DOMAINS

Capability Assessment MEA03

MEA03—*Managed Compliance with External Requirements*				
No	**Governance Practice**	**Achievement**	**Capability Level**	**Target**
1	MEA03.01 *Identify external compliance requirements.*	100% F (*Fully*)	2	4
		83% L (*Largely)*	3	
2	MEA03.02 *Optimize response to external requirements.*	100% F (*Fully*)	3	
3	MEA03.03 *Confirm external compliance.*	100% F (*Fully*)	3	
		0% N (*None*)	4	
4	MEA03.04 *Obtain assurance of external compliance.*	100% F (*Fully*)	2	
		50% P (*Partially*)	3	
		100% F (*Fully*)	4	

Capability Assessment MEA04

MEA04—*Managed Assurance*				
No	**Governance Practice**	**Achievement**	**Capability Level**	**Target**
1	MEA04.01 *Ensure that assurance providers*	100% F (*Fully*)	2	3
2	MEA04.02 *Develop risk-based planning of assurance initiatives.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
3	MEA04.03 *Determine the objectives of the assurance initiative.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
4	MEA04.04 *Define the scope of the assurance initiative.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
5	MEA04.05 *Define the work program for the assurance initiative.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
6	MEA04.06 *Execute the assurance initiative, focusing on design effectiveness*	100% F (*Fully*)	2	
		75% L (*Largely*)	3	
7	MEA04.07 *Execute the assurance initiative*	100% F (*Fully*)	3	
8	MEA04.08 *Report and follow up on the assurance initiative.*	100% F (*Fully*)	2	
		100% F (*Fully*)	3	
9	MEA04.09 *Follow up on recommendations and actions.*	100% F (*Fully*)	2	

GAP ANALYSIS AND RECOMMENDATION DESIGN

Gap Analysis

No	Governance Practice	Gap
1	MEA03.01 *Identify external compliance requirements.*	There is no integrated register that covers all external compliance requirements from all areas centrally at the organizational level.
2	MEA03.03 *Confirm external compliance.*	There is no formal mechanism to review recurring patterns of non-compliance, and no evaluation of lessons learned from previous instances of non-compliance.
3	MEA03.04 *Obtain assurance of external compliance.*	There is no integrated enterprise-wide reporting system related to compliance with legal, regulatory, and contractual obligations, so reporting management is still fragmented in each field.
4	MEA04.06 *Execute the assurance initiative, focusing on design effectiveness*	There is no evaluation mechanism or document that compares the costs and resources used in implementing management controls with the benefits or effectiveness resulting from these controls (Cost-Benefit Analysis).

Recommendation People Aspect

- Responsibility Category

No	Role	Skill	Responsibility
1	Planning and Reporting Team (Secretariat)	*Information management* (IRMG) – Level 5	- Inventory and manage external compliance registers centrally at the organizational level. - Manage compliance reporting centrally so that it is no longer managed separately between fields.
		Audit (AUDT) – Level 4	Regularly review recurring patterns of non-compliance and compile learning reports from previous instances of non-compliance.
2	*Control Owner*	*Investment appraisal* (INVA) – Level 5	Conduct a cost-benefit analysis of the implementation and maintenance of management controls, to consider the efforts and costs incurred in maintaining the continuity of controls.

GAP ANALYSIS AND RECOMMENDATION DESIGN

Recommendation Process Aspect

- Skills & Awareness Category

No	Recommendation	Skills	Training and Certification
1	Conduct compliance-related training.	Ability to detect and analyze patterns of non-compliance, identify root causes, and develop learning-based recommendations to prevent recurrence.	1. ISO 37301 *Compliance Management System* 2. CRCM (*Certified Regulatory Compliance Manager*) 3. CISA (*Certified Information Systems Auditor*)
2	Condusct training programs related to internal control.	Skills in assessing control effectiveness, cost-benefit analysis, and justifying investments in internal controls in an efficient and strategic manner.	1. CCSA (*Certification in Control Self-Assessment*) 2. COSO *Internal Control Certificate* *3. Investment Appraisal & Cost-Benefit Analysis Workshop*

- Procedure Category

No	Recommendation
MEA03—*Managed Compliance with External Requirements*	
1	Develop Integrated External Compliance Register Management Procedure
2	Develop Non-Compliance Incident Review and Learning Evaluation Procedure
3	Develop Integrated Compliance Reporting Procedure
MEA04—*Managed Assurance*	
1	Develop Control Effectiveness Evaluation Procedures Based on Cost-Benefit Analysis

GAP ANALYSIS AND RECOMMENDATION DESIGN

Recommendation
Technology Aspect

- Record Category

No	Recommendation
MEA03—*Managed Compliance with External Requirements*	
1	Compile a Report on the Results of the Evaluation of Noncompliance Incident Patterns and Lessons Learned
MEA04—*Managed Assurance*	
2	Compile a Report on the Results of the Cost-Benefit Analysis of Management Controls

- Tools Category

No	Recommendation	Tools	Description
1	Use tools that provide compliance registers to record and manage all external requirements from various fields in a centralized and structured manner.	Eramba	Eramba is an open-source GRC (Governance, Risk, Compliance) platform that provides a Compliance Management Module that supports the import of various compliance packages (e.g. ISO, NIST).
2	Use tools that can record incidents of non-compliance and analyze trends of repeat offenses.	Eramba	The Incident Management module in Eramba enables recording of non-compliance incidents as well as analysis of violation trends. It provides reporting and analytics to support continuous improvement.
3	Use tools that enable centralized compliance reporting.	Eramba	Eramba supports centralized compliance reporting through a dashboard. The reporting system is customizable and supports notifications and real-time monitoring of compliance status.
4	Use digital logging tools to help calculate and assess the efficiency of management controls based on data on costs, resources, and benefits generated (Cost-Benefit Analysis).	Google Sheets, Microsoft Excel	Google Sheets and Microsoft Excel can be used to record and analyze cost, resource, and benefit data on control implementation. Both support automated calculations, graphs, and simple modeling that are useful in conducting control efficiency evaluation and cost-benefit analysis.

ESTIMATED EFFECT OF DESIGN

No	Governance Practice	Capability Level Before Improvement	Capability Level After Improvement
EDM01: *Ensured Governance Framework Setting and Maintenance*			
1	EDM01.01 *Evaluate the governance system.*	3	3
2	EDM01.02 *Direct the governance system.*	3	3
3	EDM01.03 *Monitor the governance system.*	3	3
Total		**9**	**9**
EDM03: *Ensured Risk Optimization*			
1	EDM03.01 *Evaluate risk management*	3	3
2	EDM03.02 *Direct risk management.*	3	3
3	EDM03.03 *Monitor risk management.*	4	4
Total		**10**	**10**
MEA03: *Managed Compliance With External Requirements*			
1	MEA03.01 *Identify external compliance requirements.*	2	4
2	MEA03.02 *Optimize response to external requirements.*	3	3
3	MEA03.03 *Confirm external compliance.*	3	4
4	MEA03.04 *Obtain assurance of external compliance.*	2	4
Total		**10**	**15**
MEA04: *Managed Assurance*			
1	MEA04.01 *Ensure that assurance providers are independent and qualified*	2	2
2	MEA04.02 *Develop risk-based planning of assurance initiatives.*	3	3
3	MEA04.03 *Determine the objectives of the assurance initiative.*	3	3
4	MEA04.04 *Define the scope of the assurance initiative.*	3	3
5	MEA04.05 *Define the work program for the assurance initiative.*	3	3
6	MEA04.06 *Execute the assurance initiative, focusing on design effectiveness*	2	3
7	MEA04.07 *Execute the assurance initiative, focusing on operating effectiveness*	3	3
8	MEA04.08 *Report and follow up on the assurance initiative.*	3	3
9	MEA04.09 *Follow up on recommendations and actions.*	2	2
Total		**24**	**25**
Total Amount		**53**	**59**
Average Capability Level		**2,78**	**3,1**

DOMAIN APO

Presentation by Dita Amalia Putri

RESULTS OF DESIGN FACTOR & CAPABILITY ASSESSMENT IN APO DOMAIN

APO domain prioritization results

No	Core Model	value
1	APO12—*Managed Risk*	90
2	APO13—*Managed Security*	55
3	APO01—*Managed I&T Management Framework*	50
4	APO03—*Managed Enterprise Architecture*	45
5	APO10—*Managed Vendors*	45

Assessment Capability APO01

No	Activity	Achievement	Level	Target
1	APO01.01 *Design the management system for enterprise I&T.*	100%	2	3
		100%	3	
2	APO01.02 *Communicate management objectives, direction and decisions made.*	100%	2	
		100%	3	
3	APO01.03 *Implement management processes (to support the achievement of governance and management objectives).*	100%	2	
		100%	3	
		N.A	4	
4	APO01.04 *Define and implement the organizational structures.*	83%	2	
		100%	3	
		N.A	4	
5	APO01.05 *Establish roles and responsibilities.*	100%	2	
		100%	3	
6	APO01.06 *Optimize the placement of the IT function*	83%	3	
7	APO01.07 *Define information (data) and system ownership*	100%	3	
8	APO01.08 *Define target skills and competencies*	100%	2	2
9	APO01.09 *Define and communicate policies and procedures.*	100%	3	3
		N.A	4	
10	APO01.10 *Define and implement infrastructure*	100%	2	2
11	APO01.11 *Manage continual improvement of the I&T management system.*	N.A	4	3
		N.A	5	

RESULTS OF DESIGN FACTOR & CAPABILITY ASSESSMENT IN APO DOMAIN

Assessment Capability APO03

No	Activity	Achievement	Level	Target
1	APO03.01 *Develop the enterprise architecture vision.*	75%	2	2
		N.A	3	
		N.A	4	
2	APO03.02 *Define reference architecture.*	N.A	3	
3	APO03.04 *Define architecture implementation.*	N.A	3	
4	APO03.05 *Provide enterprise architecture services.*	N.A	3	
5	APO01.05 *Establish roles and responsibilities.*	N.A	3	
		N.A	4	
		N.A	5	

Assessment Capability APO10

No	Activitiy	Achievement	Level	Target
1	APO10.01 *Identify and evaluate vendor relationships and contracts.*	N.A	3	2
		N.A	4	
		N.A	5	
2	APO10.02 *Select vendors*	67%	2	
		N.A	3	
3	APO10.03 *Manage vendor relationships and contracts.*	N.A	3	
		N.A	4	
		N.A	5	
4	APO10.04 *Manage vendor risk.*	N.A	3	
		N.A	4	
5	APO10.05 *Monitor vendor performance and compliance.*	N.A	3	
		N.A	4	
		N.A	5	

RESULTS OF DESIGN FACTOR & CAPABILITY ASSESSMENT IN APO DOMAIN

Assessment Capability APO12

No	Activity	Achievement	Level	Target
1	APO12.01 *Collect data.*	100%	2	4
		75%	3	
		88%	4	
2	APO12.02 *Analyze risk.*	100%	3	
		50%	4	
		N.A	5	
3	APO12.03 *Maintain a risk profile.*	100%	2	
		100%	3	
		100%	4	
4	APO12.04 *Articulate risk.*	100%	3	
		100%	4	
5	APO12.05 *Define a risk management action portfolio.*	100%	2	3
		50%	3	
6	APO12.06 *Respond to risk.*	100%	3	4
		50%	4	
		N.A	5	

Assessment Capability APO13

No	Activity	Achievement	Level	Target
1	APO13.01 *Establish and maintain an*	93%	2	2
2	APO13.02 *Define and manage an information security and*	75%	3	3
		N.A	4	
3	APO13.03 *Monitor and review the information*	N.A	4	
		N.A	5	

GAP AND DESIGN RECOMMENDATIONS

GAP Analysis

No	Activity	*Level Capability Existing*	*Level Capability Targeting*	*GAP*
1	APO01.04 Define and implement the organizational structures.	3	3	There is no formal documentation such as a RACI matrix or Decision structure that explicitly defines roles and responsibilities.
2	APO01.06 Optimize the placement of the IT function.	2	3	Evaluation of deployment options and management models has not been explicitly documented.
3	APO03.01 Develop the enterprise architecture vision.	2	2	There is no explicit discussion of organizational capabilities and goals
4	APO10.02 Select vendors	2	2	There is still no request for RFIs and RFPs.
5	APO12.01 Collect data.	4	4	There is no documented and standardized service request model to support self-service and efficiency of routine requests There is no systematic identification of specific conditions affecting risk frequency and impact
6	APO12.02 Analyze Risk	3	4	There is no explicit system for validating the calibration of risk estimates.
7	APO12.06 Respond to risk.	3	4	No formal documentation is available to compare loss exposure against risk tolerance thresholds.
8	APO13.01 Establish and maintain an information security management	2	2	The ISMS approach has not been thoroughly communicated to all units
9	APO13.02 Define and manage an information security and privacy risk treatment plan.	3	3	Information security and privacy procedures have not been fully integrated across work units

People Aspect

- Skill & Awareness Category

Recommendation	Skill	Title Training and Socialization	Organizer Objective
Provide training to procurement teams on RFI/RFP preparation and evaluation procedures in accordance with SPBE guidelines and IT best practices.	*Procurement and RFP Management* (SFIA:SOUR)	*Certified in Risk and Information* (CRISC)	Improve governance and risk management capabilities in the IT procurement process.
		Certified Government Procurement Professional (CGPP)	Standardize the competence of the apparatus in the procurement of goods and services in the public sector.
		Digital Government Procurement & Vendor Management (Bappenas/SPBE)	Provide an understanding of the principles of transparency, accountability, and the use of IT in procurement.
		Certified ScrumMaster (CSM)	Promote agile-based digital procurement project management in digital transformation projects.

GAP AND DESIGN RECOMMENDATIONS

- Communication Category

No	Recommendation
1	Conduct periodic and interactive training on ISMS for all work units, with certified facilitators in the field of information security.
2	Developed a digital-based cross-unit communication program, such as a discussion forum using the MS Teams collaborative application.
3	Establish Security Awareness in each work unit as a liaison for ISMS information and security incident reporting.
4	Holding quarterly Cybersecurity Townhall Meetings involving regional leaders, SPBE management officials, and ASN representatives to deliver updates on risks, incidents, and security innovations.

- Responsibility Category

No	Recommendation
APO01 — *Managed I&T Management Framework*	
1	Develop and document procedures for evaluating the placement model and management of the IT function periodically as a reference for organizational design.
APO10 — *Managed Vendors*	
2	Develop explicit and systematic procedures for identifying risk conditions and calibrating risk estimation methods.
3	Formulating procedures for the regular validation and calibration of risk estimation results to ensure the accuracy and consistency of risk analysis.
APO13 — *Managed Security*	
4	Developing and integrating information security and privacy procedures across units to ensure coordinated planning and monitoring.

- Roles Category

No	*Skill Area*	*Level*	*Practice*	Recommendation
1	*Enterprise and Business Architecture* (ARCH)	6	APO01.06-2	Adding the role of Digital Systems and Services Planning Staff under the E-Government division to manage the coordination of IT function placement and architecture integration.
2	*Risk Management* (BURM)	5	APO12.06-3	Adding the role of IT Risk Management Staff under the Cyber and Information Security Division to handle the analysis and reporting of risk exposure against the organization's tolerance thresholds.

GAP AND DESIGN RECOMMENDATIONS

Process Aspect

- Procedure Category

No	Recommendation
APO01 — *Managed I&T Management Framework*	
1	Develop procedures for evaluating the placement and management model of IT functions
APO10 — *Managed Vendors*	
2	Develop and document RFI/RFP procedures for vendor selection based on SPBE guidelines
APO12 — *Managed Risk*	
3	Develop standardized and documented self-service request procedures
4	Develop risk identification and calibration procedures to improve estimation accuracy
5	Implement documented validation procedures for risk estimation results
6	Implement procedures to compare risk exposure with organizational tolerance thresholds
APO13 — *Managed Security*	
7	Develop and integrate information security and privacy procedures across organizational units

Technology Aspect

- Tools Category

No	Recommendation
APO10 — *Managed Vendors*	
1	Utilize an e-procurement management system that supports the creation, distribution, and evaluation of RFI/RFP documents digitally.
APO13 — *Managed Security*	
2	Implement Security Information and Event Management (SIEM) tools to enable real-time integrated security monitoring across units, support incident detection, log analysis, and security reporting.

ESTIMATED EFFECT OF DESIGN

No	Activity	Capability Level Before Design Recommendation	Capability Level After Design Recommendation
APO01 — *Managed I&T Management Framework*			
1	APO01.01 *Design the management system for enterprise I&T.*	3	3
2	APO01.02 *Communicate management objectives, direction and decisions made.*	3	3
3	APO01.03 *Implement management processes*	3	3
4	APO01.04 *Define and implement the organizational structures.*	3	3
5	APO01.05 *Establish roles and responsibilities002E*	3	3
6	APO01.06 *Optimize the placement of the IT function.*	2	3
7	APO01.07 *Define information (data) and system ownership.*	3	3
8	APO01.08 *Define target skills and competencies.*	2	2
9	APO01.09 *Define and communicate policies and procedures.*	3	3
10	APO01.10 *Define and implement infrastructure, services and applications to support the governance and management system.*	2	2
11	APO01.11 *Manage continual improvement of the I&T management system.*	N.A	N.A
Total		27	28

APO03 — *Managed Enterprise Architecture*			
12	APO03.01 *Develop the enterprise architecture vision.*	2	2
13	APO03.02 *Define reference architecture.*	N.A	N.A
14	APO03.03 *Select opportunities and solutions.*	N.A	N.A
15	APO03.04 *Define architecture implementation.*	N.A	N.A
16	APO03.05 *Provide enterprise architecture services.*	N.A	N.A
Total		2	2
APO10 — *Managed Vendors*			
17	APO10.01 *Identify and evaluate vendor relationships and contracts.*	N.A	N.A
18	APO10.02 *Select vendors*	1	2
19	APO10.03 *Manage vendor relationships and contracts.*	N.A	N.A
20	APO10.04 *Manage vendor risk.*	N.A	N.A
21	APO10.05 *Monitor vendor performance and compliance.*	N.A	N.A
Total		1	2

APO12 — *Managed Risk*			
22	APO12.01 *Collect data.*	2	4
23	APO12.02 *Analyze risk.*	3	4
24	APO12.03 *Maintain a risk profile.*	4	4
25	APO12.04 *Articulate risk.*	4	4
26	APO12.05 *Define a risk management action portfolio.*	3	4
27	APO12.06 *Respond to risk.*	3	4
Total		19	24
APO13 — *Managed Security*			
28	APO13.01 *Establish and maintain an information security management system (ISMS).*	1	3
29	APO13.02 *Define and manage an information security and privacy risk treatment plan.*	2	3
30	APO13.03 *Monitor and review the information security management system (ISMS).*	N.A	N.A
Total		3	6
Total amount		52	62
Skor Total		**2,74**	**3,26**

DOMAIN BAI

Presentation by Gaitsa Zahira Shafa

RESULTS OF DESIGN FACTOR & CAPABILITY ASSESSMENT IN BAI DOMAIN

BAI domain prioritization results

No	***Governance and Management Objectives*** **(GMO)**	Score
1	BAI11: *Managed Projects*	100
2	BAI01: *Managed Programs*	70
3	BAI04: *Managed Availability & Capability*	70
4	BAI03: *Managed Solutions Identification & Build*	60

Assessment Capability BAI01

BAI01 – *Managed Programs*				
No.	**Management Practices**	**Capability Level**	**Achievement**	**Target**
1	BAI01.01 Maintain a standard approach for program management.	2	100%	3
		3	100%	
		4	N.A.	
2	BAI01.02 Initiate a program.	2	100%	3
		3	100%	
3	BAI01.03 Manage stakeholder engagement.	3	100%	3
		4	N.A.	
4	BAI01.04 Develop and maintain the program plan.	2	100%	3
		3	90%	
5	BAI01.05 Launch and execute the program.	3	100%	3
		4	N.A.	
6	BAI01.06 Monitor, control and report on the program outcomes.	3	100%	3
		4	N.A.	
7	BAI01.07 Manage program quality.	3	75%	3
		4	N.A.	
8	BAI01.08 Manage program risk.	3	100%	3
9	BAI01.09 Close a program.	3	100%	3
		4	N.A.	
		5	N.A.	

BAI03 – *Managed Solutions Identification Build*				
No.	**Management Practices**	**Capability Level**	**Achievement**	**Target**
1	BAI03.01 Design high-level solutions.	2	100%	2
2	BAI03.02 Design detailed solution components.	2	92%	3
		3	100%	
3	BAI03.03 Develop solution components.	2	100%	3
		3	100%	
4	BAI03.04 Procure solution components.	3	100%	3
5	BAI03.05 Build solutions.	2	100%	3
		3	90%	
6	BAI03.06 Perform quality assurance (QA).	3	100%	3
		4	N.A.	
7	BAI03.07 Prepare for solution testing.	2	100%	3
		3	100%	
8	BAI03.08 Execute solution testing.	2	100%	2
9	BAI03.09 Manage changes to requirements.	3	100%	3
10	BAI03.10 Maintain solutions.	2	100%	3
		3	100%	
		4	N.A.	
11	BAI03.11 Define IT products and services and maintain the service portfolio.	3	88%	3
12	BAI03.12 Design solutions based on the defined development methodology.	3	100%	3

Assessment Capability BAI03

Assessment Capability BAI04

BAI04 – *Managed Availability and Capacity*				
No.	**Management Practices**	**Capability Level**	**Achievement**	**Target**
1	BAI04.01 Assess current availability, performance and capacity and create a baseline.	2	100%	3
		3	100%	
		4	N.A.	
2	BAI04.02 Assess business impact.	2	100%	3
		3	100%	
		4	N.A.	
3	BAI04.03 Plan for new or changed service requirements.	3	50%	3
		4	N.A.	
		5	N.A.	
4	BAI04.04 Monitor and review availability and capacity.	2	100%	3
		3	100%	
		4	N.A.	
5	BAI04.05 Investigate and address availability, performance and capacity issues.	3	100%	3
		4	N.A.	
		5	N.A.	

RESULTS OF DESIGN FACTOR & CAPABILITY ASSESSMENT IN BAI DOMAIN

BAI11 – *Managed Projects*				
No.	**Management Practices**	**Capability Level**	**Achievement**	**Target**
1	BAI11.01 Maintain a standard approach for project management.	2	100%	4
		3	100%	
		4	100%	
2	BAI11.02 Start up and initiate a project.	2	100%	2
3	BAI11.03 Manage stakeholder engagement.	3	100%	4
		4	100%	
4	BAI11.04 Develop and maintain the project plan.	2	100%	2
5	BAI11.05 Manage project quality.	2	100%	3
		3	100%	
6	BAI11.06 Manage project risk.	2	100%	3
		3	100%	
7	BAI11.07 Monitor and control projects.	2	100%	4
		3	100%	
		4	100%	
8	BAI11.08 Manage project resources and work packages.	2	93%	2
9	BAI11.09 Close a project or iteration.	2	100%	4
		3	100%	
		4	100%	

Assessment
Capability
BAI11

GAP AND DESIGN RECOMMENDATIONS

Gap Analysis

No.	Governance Practice	Gap
1	BAI01.04 Develop and maintain the program plan.	No formal plan to create a business case and list of benefits
2	BAI01.07 Manage program quality.	Not yet a complete process for identifying and developing new or modified systems
3	BAI03.02 Design detailed solution components.	Lack of detail in the definition of data and use cases
4	BAI03.05 Build solutions.	Lack of optimal integration between data and information systems
5	BAI03.11 Define IT products and services and maintain the service portfolio.	Lack of detailed documentation related to product portfolio
6	BAI04.03 Plan for new or changed service requirements.	Lack of data analysis collection, leading to a lack of in-depth understanding of how business needs
7	BAI11.08 Manage project resources and work	Delays in the repair or remediation process of the project plan

Recommendation People Aspect

- Responsibility Category

No.	Role	Skill	Responsibility
BAI01.04			
1	Business Case Manager	Responsible for the maintenance of business case and benefit lists	- Establish a business case planning and update process - Ensure maintenance of the benefits list - Conduct regular evaluation of business case progress
BAI03.02			
2	Use Case Designer	Manage and define data and use cases	- Establish data management standards - Develop clear definitions for each use case - Periodically verify data and test use cases

GAP AND DESIGN RECOMMENDATIONS

Recommendation People Aspect

- Skill & Awareness Category

No.		Recommendation	Skill	Training and Certification
1	BAI01.07	Conduct skills training to identify and evaluate new systems related to internal controls and security	Security and Risk Management	1. System Security and Risk Management Training 2. CISSP certification (Certified Information Systems Security Professional)
2	BAI03.05	Conduct training related to the design and implementation of integration solutions between data and systems	System Integration & Architecture	1. System Integration and Architecture Training 2. TOGAF certification (The Open Group Architecture Framework) Certification
3	BAI03.11	Conduct awareness training on the importance of standardized documentation and long-term project goals	Documentation & Project Management	1. Documentation and Product Portfolio Management Training 2. PMP certification (Project Management Professional) Certification
4	BAI04.03	Organizing training on capacity analysis and the use of modeling tools related to business needs	Capacity Planning & Data Analysis	1. IT Capacity Analysis Training 2. ITIL certification (Information Technology Infrastructure Library) Certification

- Communication Category

No	Recommendation
BAI11.08	
1	Give more trust to the team to take temporary decisions in certain conditions
2	Conduct meetings or discussions on a weekly basis to ensure problems are identified more quickly

GAP AND DESIGN RECOMMENDATIONS

Recommendation Process Aspect

- Policy Category

No.		Policy	Responsibility	Description
1	BAI01 .07	System management and security policy	- Establish policies for identifying, evaluating, and modifying systems	The policy aims to ensure that any new or modified systems are subjected to a security evaluation process and verification of internal controls in accordance with established standards.
2	BAI03 .05	Data and system integration policy	- Establish policies for integrating data and systems by ensuring interoperability between solution components	This policy ensures that any system and data integration is prioritized and performed in accordance with established technical standards to achieve effective interoperability between components.
3	BAI03 .11	Product portfolio documentation policy	- Establish policies that ensure complete documentation for each product or service managed	This policy ensures that each product and service is recorded in detail in up-to-date portfolio documentation.
4	BAI04 .03	Capacity and business needs analysis policy	- Establish policies that require system capacity analysis to be conducted on a regular basis	This policy ensures capacity analysis and a better understanding of the impact of changing business needs and improves the team's understanding of how to respond to change.
5	BAI11 .08	Quick decision-making and follow-up policy	- Establish policies to make quick decisions on issues that arise in the project	This policy ensures that any issues in the project can be dealt with quickly (temporarily), immediate feedback is given to avoid delays, and keep the project on track.

- Procedure Category

No	Recommendation
BAI01.04	
1	Develop SOPs to document in detail each step in business case planning and maintenance.
BAI03.02	
2	Develop an SOP to develop data specifications by detailing the types of data, data sources, and relationships between data.

Recommendation Technology Aspect

- Tools Category

No	Recommendation
BAI01.04	
1	Use Google Sheets to create, document, and monitor business cases and benefit lists
BAI01.07	
2	Use ServiceNow to identify, monitor and manage internal controls and security solutions on new or modified systems

ESTIMATED EFFECT OF DESIGN

No.	Activity	Capability Level Before Improvement	Capability Level After Improvement
BAI01 - *Managed Programs*			
1	BAI01.01 *Maintain a standard approach for program management.*	3	3
2	BAI01.02 *Initiate a program.*	3	3
3	BAI01.03 *Manage stakeholder engagement.*	3	3
4	BAI01.04 *Develop and maintain the program plan.*	3	3
5	BAI01.05 *Launch and execute the program.*	3	3
6	BAI01.06 *Monitor, control and report on the program outcomes.*	3	3
7	BAI01.07 *Manage program quality.*	3	3
8	BAI01.08 *Manage program risk.*	3	3
9	BAI01.09 *Close a program.*	3	3
Total		**27**	**27**

BAI03 - *Managed Solutions Identification and Build*			
1	BAI03.01 *Design high-level solutions.*	2	2
2	BAI03.02 *Design detailed solution components.*	3	3
3	BAI03.03 *Develop solution components.*	3	3
4	BAI03.04 *Procure solution components.*	3	3
5	BAI03.05 *Build solutions.*	3	3
6	BAI03.06 *Perform quality assurance (QA).*	3	3
7	BAI03.07 *Prepare for solution testing.*	3	3
8	BAI03.08 *Execute solution testing.*	2	2
9	BAI03.09 *Manage changes to requirements.*	3	3
10	BAI03.10 *Maintain solutions.*	3	3
11	BAI03.11 *Define IT products and services and maintain the service portfolio.*	3	3
12	BAI03.12 *Design solutions based on the defined development methodology.*	3	3
Total		**34**	**34**

BAI04 - *Managed Availability and Capability*			
1	BAI04.01 *Assess current availability, performance and capacity and create a baseline.*	3	3
2	BAI04.02 *Assess business impact.*	3	3
3	BAI04.03 *Plan for new or changed service requirements.*	2	3
4	BAI04.04 *Monitor and review availability and capacity.*	3	3
5	BAI04.05 *Investigate and address availability, performance and capacity issues.*	3	3
Total		**14**	**15**
BAI11 - *Managed Projects*			
1	BAI11.01 *Maintain a standard approach for project management.*	4	4
2	BAI11.02 *Start up and initiate a project.*	2	2
3	BAI11.03 *Manage stakeholder engagement.*	4	4
4	BAI11.04 *Develop and maintain the project plan.*	2	2
5	BAI11.05 *Manage project quality.*	3	3
6	BAI11.06 *Manage project risk.*	3	3
7	BAI11.07 *Monitor and control projects.*	4	4
8	BAI11.08 *Manage project resources and work packages.*	2	2
9	BAI11.09 *Close a project or iteration.*	4	4
Total		**28**	**28**
Total Amount		**103**	**104**
Avarage Capability Level		**2,94**	**2,97**

CONCLUSION

EDM & MEA Domain

- The initial IT governance capability level at XYZ Provincial government was at level 2.78, based on the identification of four priority objectives - EDM01, EDM03, MEA03, and MEA04 - indicating gaps in some management practices.
- The IT Governance Design using the COBIT 2019 framework (EDM & MEA domains) resulted in 19 recommendations on people, process and technology aspects, which could potentially improve capability to level 3.10 if implemented.

APO Domain

- Most IT governance processes such as APO01, APO03, APO10, APO12, and APO13 in XYZ Province remain at capability level 1–2.
- Governance gaps exist in documentation, architecture, vendor management, and security, requiring structured improvement.
- A roadmap of 9 initiatives was proposed to gradually elevate capabilities to level 3 and support sustainable digital transformation.

BAI Domain

- In the existing condition of IT governance, there are 4 highest values which are the main focus of research, namely, BAI11 with a value of 100, BAI01 with a value of 70, BAI04 with a value of 70 and BAI03 with a value of 60.
- Results in gaps between existing conditions and established standards that need to be improved in 4 BAI domains.
- Resulted a total of 16 recommendations on people, process and technology aspects that can improve the company's digital transformation.

Telkom University

Fakultas Rekayasa Industri
Telkom University

THANK YOU