

# An Analysis of Information Technology Governance Using COBIT 2019: A Case Study of the ICT Unit at Tadulako University

Magfirah Di'iznania Armin<sup>1</sup>, Hamzah Ritchi<sup>2</sup>, Nanny Dewi Tanzil<sup>3</sup>

<sup>1,2,3</sup>Faculty of Economics and Business, Universitas Padjadjaran, Indonesia

## Abstract

*The rapid advancement of information technology (IT) requires educational institutions to implement effective IT governance aligned with organizational business strategies and operations. This study aims to evaluate the capability level of IT governance at the Information and Communication Technology Unit (UPT TIK) of Tadulako University using the COBIT 2019 framework, with a focus on two specific processes: APO12 (Managed Risk) and APO13 (Managed Security). A mixed-methods approach was employed, including data collection through observations, interviews, and questionnaires. The Guttman scale and capability level calculations were used for analysis. The findings indicate that the current capability level for APO12 is at level 2, and APO13 is at level 1, whereas the desired target for both is level 4. This significant gap highlights the need for improvements in IT governance. Strategic recommendations based on the COBIT 2019 guidelines are proposed to help the institution achieve its target capability levels.*

## Keywords

IT Governance, COBIT 2019, APO12, APO13, Capability Level, Tadulako University



## I. Introduction

Information Technology (IT) has become a critical enabler in supporting the operational performance and strategic goals of organizations, including higher education institutions. Effective IT governance contributes to improving productivity, service quality, and decision-making through proper alignment between IT and business objectives (De Haes & Van Grembergen, 2009; ISACA, 2018).

Tadulako University, a public university located in Palu, Indonesia, has implemented various IT systems to support academic and administrative activities through the Information and Communication Technology Unit (UPT TIK). This unit is responsible for managing IT services and infrastructure within the university. However, challenges persist, such as the lack of an optimal organizational structure, insufficient skilled personnel, and underdeveloped information security practices. These issues reflect the common struggle in higher education institutions where IT governance is not yet fully institutionalized (Alreemy et al., 2016).

UPT TIK's vision is to serve as a data management and IT service center that supports the university's tridharma (education, research, and community service). To achieve this, the unit must adopt structured standards and policies to govern its operations. Good IT governance not only enhances operational excellence but also reduces waste, inefficiency, and financial risks (Lunardi et al., 2014). Poor governance, on the other hand, can lead to delayed services, fragmented systems, and security vulnerabilities (Weill & Ross, 2004).

Despite efforts to digitize processes, Tadulako University still faces issues such as unstable networks, outdated software, and delays in web-based communication caused by staff turnover and lack of documentation. These weaknesses indicate a need for structured and sustainable IT governance mechanisms (Mangalaraj & Parameswaran, 2014).

To address these challenges, the COBIT (Control Objectives for Information and Related Technologies) framework, developed by ISACA, offers a comprehensive set of globally recognized IT governance practices. COBIT is designed to help organizations bridge the gap between control requirements, technical issues, and business risks (ISACA, 2018). COBIT 2019, in particular, is known for its flexibility and adaptability to current technology trends, making it suitable for dynamic environments such as universities (ISACA, 2019).

Several studies have adopted COBIT to assess IT governance maturity. For example, Salegar and Rizal (2020) evaluated the academic information system governance in Indonesian universities using COBIT 5, finding a maturity level of 3 (established). Nachrowi et al. (2020), using COBIT 2019, revealed that many higher education governance processes remain at levels 0 or 1. Belo et al. (2020) applied COBIT 2019 in a large telecommunications company, identifying critical areas needing structured governance interventions.

The assessment is expected to provide insights into the current governance level and formulate actionable recommendations for improvement. While various IT systems have been implemented, several issues remain. These include underdeveloped human resource capabilities, staff shortages during organizational transitions, delays in website updates, unstable network infrastructure, and software misalignment with organizational needs. Furthermore, the organizational structure within UPT TIK lacks clear role definitions, which inhibits the effective assignment of responsibilities critical to IT governance and management processes.

In response to these challenges, the COBIT (Control Objectives for Information and Related Technologies) framework developed by ISACA (2018) is considered an appropriate tool for evaluating and improving IT governance. COBIT provides a set of best practices and standardized processes that guide management, auditors, and IT professionals in bridging the gap between business risks, technical challenges, and control requirements (Mangalaraj, 2014).

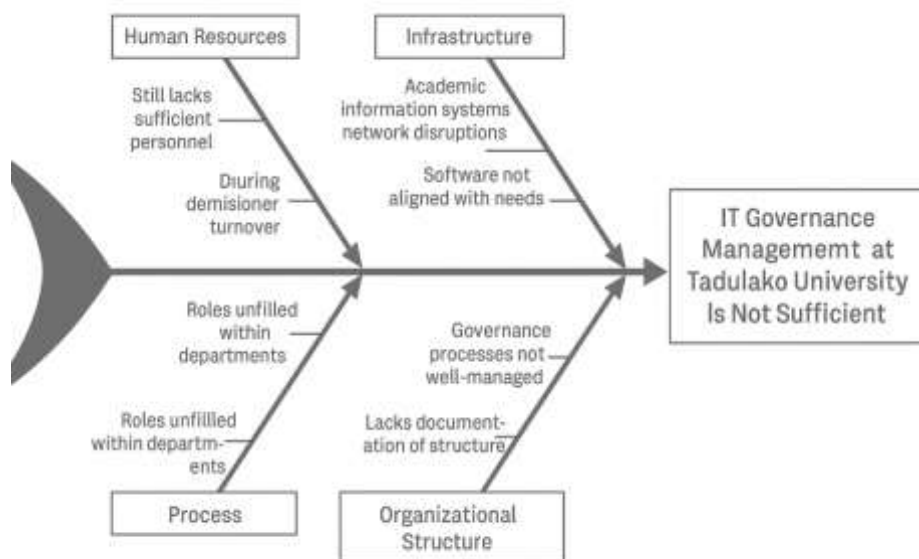
Other researchers have applied COBIT 2019 in different contexts. Belo et al. (2020) used the framework to design IT governance in a regional branch of PT Telekomunikasi Indonesia, identifying 14 essential processes for business continuity. In the healthcare sector, Nasution et al. (2021) assessed IT governance in a government hospital, revealing the importance of aligning IT strategy with service delivery. Fitri et al. (2022) analyzed IT governance in a private university using COBIT 2019 and found low maturity in risk and security processes, recommending structural improvements. Additionally, Rahmatillah and Nugroho (2022) highlighted the role of COBIT 2019 in assessing governance for cloud-based learning management systems, stressing the importance of aligning digital infrastructure with academic goals. Ahmad et al. (2021) compared COBIT 5 and COBIT 2019 in public sector organizations, concluding that COBIT 2019 is more adaptable due to its design factor approach.

While these studies demonstrate the practical use of COBIT frameworks, most focus broadly on institutional governance or system maturity. Few have focused specifically on APO12 (Managed Risk) and APO13 (Managed Security)—two critical processes related to institutional resilience and information security. Given Tadulako University's challenges in risk mitigation and IT security management, this research seeks to evaluate the current

capability levels of APO12 and APO13 using the COBIT 2019 framework and provide strategic recommendations to bridge identified gaps.

Based on the review of previous studies, it can be concluded that one of the most widely adopted and effective frameworks for evaluating the maturity level of IT governance is the COBIT 2019 framework. The primary reason for selecting COBIT 2019 in this study is its flexibility and adaptability to the current trends and rapid developments in information technology. In contrast to its predecessors, COBIT 2019 incorporates dynamic governance design factors and is better aligned with modern IT management frameworks such as ITIL, TOGAF, and ISO/IEC standards, making it highly applicable across various organizational contexts (ISACA, 2019).

To better understand the root causes of ineffective IT governance at Tadulako University, a root cause analysis was conducted using a Fishbone Diagram (also known as an Ishikawa Diagram). This method allows for a systematic identification of key contributing factors that lead to suboptimal performance in IT governance implementation. The analysis focuses on four primary categories: Human Resources, Infrastructure, Processes, and Organizational Structure. Each category highlights specific issues that have been observed during the study, including personnel shortages, unstable network infrastructure, unfilled departmental roles, and lack of formal governance documentation. By visually mapping these problems, the diagram provides a clear overview of the critical weaknesses that must be addressed to improve the university's IT governance capability. Figure 1 illustrates this analysis.



**Figure 1. Fishbone Diagram**

Figure 1 presents a Fishbone Diagram (Ishikawa Diagram) that illustrates the root causes of inadequate IT governance at Tadulako University. The central issue identified is insufficient IT governance management, caused by deficiencies across four key areas: Human Resources, Infrastructure, Processes, and Organizational Structure. In the human resources category, the university suffers from a lack of qualified IT staff and role discontinuities caused by leadership transitions. This aligns with recent findings by Fitri et al. (2022), who emphasized that human capital plays a critical role in determining IT governance capability levels in higher education institutions.

From an infrastructure perspective, unstable network connections and the use of outdated or misaligned software hinder system efficiency and service delivery. Rahmatillah and Nugroho (2022) argue that poor alignment between IT infrastructure and organizational needs significantly delays digital transformation efforts in universities. The “Processes” category shows that several functional units experience role vacancies, which limits coordination and responsiveness. This echoes the conclusions of Nasution et al. (2021), who found that weak process execution and unfilled IT roles contribute to poor service quality and slow risk response times.

Lastly, under “Organizational Structure,” the absence of a clearly documented structure and undefined responsibilities has led to governance ambiguity and lack of accountability. Ahmad et al. (2021) highlight that without a structured governance framework such as COBIT 2019, universities often struggle to assign ownership and enforce IT controls effectively. These interconnected issues point to the need for a comprehensive restructuring and strategic alignment of IT governance processes at Tadulako University, in line with modern governance models and national digital education goals.

In light of the aforementioned background, it can be concluded that the management of Information Technology (IT) at Tadulako University is still insufficient and requires significant improvement. Several indicators support this assessment: First, the quality of human resources (HR) within the university remains inadequate, particularly in terms of IT governance capabilities. Many personnel lack the necessary technical and managerial skills to support IT systems effectively. Second, staff shortages frequently occur during transitions of unit leadership (demissioner phase). These shortages particularly affect units responsible for maintaining official websites, resulting in frequent delays in updating institutional information—an issue that directly impacts communication transparency and user satisfaction. Third, the organizational structure of the ICT Unit (UPT TIK) has not yet been clearly defined. The absence of detailed role descriptions and formal documentation makes it difficult to assign responsibilities, measure accountability, and streamline governance processes. Improving the organizational structure is therefore seen as a crucial step in advancing the effectiveness of IT management. Fourth, the university continues to face issues related to academic information systems, including frequent network instability and the use of software solutions that do not align with actual operational needs. These technical obstacles hinder the seamless delivery of services and compromise system reliability.

Despite these challenges, Tadulako University aspires to strengthen its IT governance framework in line with best practices. In accordance with Article 16, Paragraph 1 of Government Regulation No. 82 of 2012, good governance of electronic systems must include comprehensive processes of planning, operation, maintenance, and documentation. The conditions outlined above indicate clear deficiencies in the university’s IT governance practices. Therefore, this research aims to assess the capability level of IT governance at Tadulako University using a structured framework. The results are expected to provide a detailed overview of the current situation and offer targeted recommendations for improving IT governance performance in alignment with institutional goals.

Accordingly, this study seeks to conduct an in-depth analysis of IT governance at Tadulako University, using the title: "An Analysis of Information Technology Governance Using COBIT 2019: A Case Study of Tadulako University, Palu, Central Sulawesi." The results of this analysis are expected to provide a detailed assessment of the current capability levels of selected IT governance processes, along with the desired target levels.

These findings will be mapped against the objectives of the organization to ensure alignment with institutional strategy and business goals. Furthermore, this study aims to offer strategic recommendations for improving the implementation, control, and utilization of IT resources within the university environment.

## **II. Review of Literatures**

In conducting this research, a strong theoretical foundation is necessary to support the analysis of IT governance implementation. A literature review helps identify key concepts, frameworks, and previous studies relevant to the governance and management of information technology. This section explores several important aspects that underpin the research, including the definition of analysis as a methodological approach, the concept and significance of IT governance, the role of the ICT Unit at Tadulako University, and the COBIT framework as the primary tool used to assess governance capabilities. Particular emphasis is placed on COBIT 2019, the most recent version of the COBIT framework developed by ISACA, which offers a structured, flexible, and modern approach to evaluating and improving IT governance in alignment with organizational goals.

### **2.1 Analysis**

Analysis is the process of breaking down a whole into its individual components to better understand the function, relationships, and roles of each part within an integrated system. Komarudin (1994) defines analysis as a cognitive activity to deconstruct a comprehensive object into its fundamental elements. Similarly, Sudjana (2016) describes analysis as the effort to break down an integrated unit into smaller parts in order to clarify its structure and hierarchy. According to the Kamus Besar Bahasa Indonesia (Great Dictionary of the Indonesian Language), analysis is the act of separating a subject into its parts and examining those parts to understand the whole.

From these perspectives, analysis can be concluded as a systematic effort to observe, deconstruct, and critically examine an object or phenomenon with the aim of discovering new insights. It involves identifying reliable evidence to support understanding and generating conclusions based on observed facts.

### **2.2 Information Technology (IT) Governance**

IT governance refers to the structures, interactions, and processes that guide and control an organization's use of IT to achieve strategic objectives. According to the IT Governance Institute (ITGI, 2007), IT governance involves consideration of value and risk arising from IT implementation and processes. Weill and Ross (2004) define IT governance as “specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT.” It establishes who has the authority to make decisions, how accountability is assigned, and how IT contributes to the organization’s goals.

ISACA (2012) states that IT governance is the responsibility of the Board of Directors and executive management, forming an integral part of overall corporate governance. It consists of leadership, organizational structures, and processes that ensure IT supports and extends the organization’s strategies and objectives. Dull and Gelinas (2008) reinforce this by emphasizing that IT governance includes processes that ensure leadership, IT structure, and technology are aligned with corporate vision and mission. Swastika (2016) further adds that IT governance is the organizational mechanism for applying IT policies and managing IT resources to ensure that technology use aligns with strategic goals.

In summary, IT governance is a managerial responsibility that ensures continuity between institutional expectations and operational performance. It synchronizes technology use with business processes so that users can work according to established procedures and goals.

### **2.3 Importance of IT Governance**

According to Weill and Ross (2004), effective IT governance ensures alignment between management decisions, business objectives, and IT utilization. Its importance is reflected in several key areas. First, good governance enables accountable, high-quality decision-making regarding IT operations. Second, it enhances management effectiveness across various areas by providing a structured framework for IT-related decisions. Third, it ensures that IT supports core organizational priorities and strategic goals. Fourth, it acts as a driver for innovation and new business opportunities. Finally, it allows organizations to extract optimal value from IT investments through disciplined, strategic governance mechanisms.

### **2.4 Principles of IT Governance Implementation**

Weill and Ross (2004) propose several principles for implementing effective IT governance. The first is clarity—the governance framework should clearly define responsibilities and goals within the organization. The second is transparency, which refers to the existence of clear processes and mechanisms accessible to all decision-makers. The third is appropriateness, which emphasizes the importance of involving competent individuals who understand the technology, the business context, and governance frameworks.

### **2.5 ICT Unit (UPT TIK) at Tadulako University**

To support its mission in education, Tadulako University established its Computer Unit on February 2, 1998, based on Rector Decree No. 420a/J28/KP/1998. The unit was created to implement the university's Tridharma Perguruan Tinggi (three pillars of higher education): education, research, and community service. As technology evolved, the unit was renamed PPTIK (Center for Information and Communication Technology Services) on January 27, 2012, through Rector Decree No. 829/UN28/KL/2012. To further improve efficiency and alignment with national higher education regulations, the unit underwent another transformation on March 21, 2013, becoming the ICT Unit (UPT TIK) based on Rector Decree No. 1826/UN28/KP/2013 and Ministry of Education and Culture Regulation No. 70 of 2012. As stated in Article 89, UPT TIK is tasked with the development, management, and provision of information and communication technology services to support academic, research, administrative, and community engagement functions at the university.

### **2.6 Benefits of IT Governance**

Weill and Vitale (2002) identified five key areas in which IT governance decisions contribute to the strategic advantage of organizations:

1. IT Principles – These are guiding statements on how IT should be used within the organization and its strategic direction. Effective IT principles foster cross-functional alignment across departments such as finance, marketing, and operations.
2. IT Architecture Decisions – This includes the logical structuring of data, infrastructure, and applications. It defines standards for integration and technology choices to achieve the desired business goals.



3. IT Infrastructure – This refers to the hardware, software, and networks that support business operations. A robust IT infrastructure improves speed, accuracy, and accessibility of information in various formats—data, images, text, and video.
4. Business Application Needs – Organizations must creatively and systematically identify how IT can create new value. This involves both creativity (to discover innovative methods) and discipline (to ensure architectural consistency).
5. IT Investment and Prioritization – Investment in IT is often hard to quantify in terms of direct return. Thus, IT governance must help decision-makers prioritize funding and ensure alignment between IT expenditure and organizational strategy.

## **2.7 COBIT (Control Objectives for Information and Related Technology)**

COBIT (Control Objectives for Information and Related Technology) is a comprehensive framework used for the governance and management of enterprise IT. Developed by the IT Governance Institute (ITGI) under the umbrella of the Information Systems Audit and Control Association (ISACA), COBIT was initially released in 1996 with an emphasis on auditing processes. The framework evolved significantly over time, with COBIT 2.0 in 1998 focusing more on governance controls, followed by COBIT 3.0 in 2000 which introduced IT management-oriented guidance.

In 2005, COBIT 4.0 was released, and subsequently COBIT 4.1 in 2007, both of which strengthened the relationship between IT governance and business goals. COBIT 5, launched in 2012, became a major milestone, offering an integrated model for the governance and management of enterprise IT, applicable to the entire organization. The most recent version, COBIT 2019, was officially released in 2018 and represents a major update that addresses new digital transformation challenges and the integration of modern technologies.

According to ITGI (2007), "COBIT is a framework and supporting toolset that allow managers to bridge the gap with respect to control requirements, technical issues, and business risks, and communicate that level of control to stakeholders." In other words, COBIT helps managers align IT processes and responsibilities with organizational goals while addressing business risks and technical concerns in a structured and communicable way.

## **2.8 COBIT 2019**

COBIT 2019, published by ISACA, is the latest iteration of the COBIT framework and is designed to help organizations govern and manage enterprise information and technology. Unlike previous versions, COBIT 2019 distinctly separates governance and management, each with its own structures, objectives, and activities. Governance focuses on evaluating stakeholder needs, setting direction through prioritization and decision-making, and monitoring performance and compliance with agreed objectives. Management, on the other hand, is responsible for planning, building, running, and monitoring IT activities in alignment with governance directions (ISACA, 2018).

COBIT 2019 enables organizations to ensure that IT contributes to strategic objectives, manages risk effectively, and delivers value. It supports a flexible and open framework, adaptable to different organizational contexts, including private and public sectors, small and medium enterprises, and large corporations undergoing digital transformation.

## 2.9 Focus Areas

Focus Areas in COBIT 2019 refer to specific topics, domains, or governance challenges that can be addressed using customized sets of governance and management objectives. Examples include cybersecurity, digital transformation, cloud computing, data privacy, DevOps, and small to medium enterprises (SMEs). Focus Areas allow organizations to tailor COBIT to their particular needs, making the framework highly scalable and adaptable. Since COBIT is an open model, new Focus Areas can be added by experts or practitioners as needed, enabling the framework to remain relevant in evolving digital environments.

## 2.10 Design Factors

Design Factors are critical elements that influence how an organization designs and scopes its IT governance system. COBIT 2019 identifies 11 Design Factors, which serve two primary purposes:

1. Factors 1–4 help determine the initial scope of the governance system,
2. Factors 5–11 help refine and tailor the system for better alignment and effectiveness.

These design factors include aspects such as enterprise strategy, goals, risk appetite, compliance requirements, IT-related issues, threat landscape, and organizational size, among others. By considering these factors, organizations can customize their governance systems and map their governance objectives to specific Focus Areas that align directly with their business strategy (ISACA, 2018). This ensures that the IT governance system is both effective and contextually relevant.



**Figure 2.** COBIT Design Factors (ISACA)

Figure 2 illustrates the structural components of the COBIT 2019 framework as introduced by ISACA (2018). At its core, COBIT 2019 is designed to provide a comprehensive governance system for enterprise information and technology. The framework is built upon two key domains: Governance and Management. The Governance domain ensures that stakeholder needs are evaluated, direction is set, and performance is monitored. In contrast, the Management domain consists of the planning, building, running, and monitoring of IT activities in alignment with strategic direction.

Surrounding these domains are several integral components:

1. Governance and Management Objectives, which represent specific, actionable processes used to achieve enterprise goals;
2. Design Factors, which influence how the governance system is tailored based on organizational context such as risk appetite, size, strategy, and regulatory requirements;



3. Focus Areas, which are thematic topics like cybersecurity, DevOps, and digital transformation, allowing the COBIT model to remain flexible and adaptable;
4. Performance Management, used to measure and assess the capability and maturity of governance implementation.

Together, these elements enable organizations to design and implement a governance system that is customizable, scalable, and aligned with business objectives. The framework's modular nature ensures that it can be adapted to a wide range of industries and enterprise needs, making it a robust tool for IT governance evaluation and improvement.

**Table 1.** Enterprise Strategy Types and Their Influence on IT Governance Design

Enterprise Strategy Type	Strategic Focus	Governance Implications
Growth / Acquisition	Business expansion, mergers, entering new markets	Requires governance structures that support agility, scalability, and innovation adoption
Innovation / Differentiation	Unique product or service offerings	Emphasizes digital transformation, R&D investment, and flexible IT project governance
Cost Leadership / Optimization	Operational efficiency, cost reduction	Focuses on standardization, automation, and risk management
Service Continuity / Risk Aversion	Stability, compliance, and disaster recovery	Requires strong control mechanisms, compliance processes, and secure infrastructure
Customer Intimacy / Responsiveness	Customer-centric approach	Demands IT systems that are responsive, personalized, and integrated with CRM
Digital Transformation	Enterprise-wide digital modernization	Prioritizes cloud adoption, cybersecurity, agile delivery models, and governance flexibility

(Adapted from ISACA, 2019)

As outlined in Table 2.1, COBIT 2019 classifies enterprise strategies into several types, each with specific implications for the design of IT governance systems. An organization that pursues a growth or acquisition strategy focuses on expansion, mergers, or entering new markets. Such a strategy requires governance structures that support agility, scalability, and innovation, ensuring that IT systems can adapt rapidly to business changes.

Enterprises focused on innovation or differentiation seek to deliver unique products or services. In this case, IT governance must enable research and development, support experimental projects, and allow for greater flexibility in managing emerging technologies. By contrast, organizations that adopt a cost leadership or optimization strategy emphasize efficiency and cost reduction. Their governance model prioritizes standardization, process automation, and risk control to reduce overhead and improve operational performance.

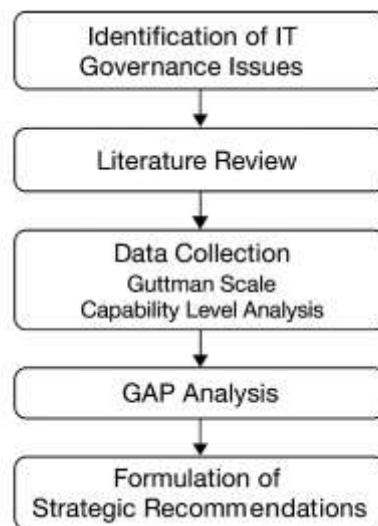
Another strategic direction is service continuity or risk aversion, which is typically adopted by institutions in highly regulated or risk-sensitive industries, such as finance or healthcare. These organizations require strict compliance frameworks, robust control mechanisms, and highly secure infrastructure to ensure uninterrupted service delivery and risk mitigation.

For businesses adopting a customer intimacy or responsiveness strategy, the focus is on creating personalized experiences and rapidly responding to customer needs. IT governance in such cases must ensure that systems are responsive, customer-oriented, and integrated with customer relationship management (CRM) tools.

Lastly, organizations undergoing digital transformation aim for enterprise-wide modernization through technology. This strategy requires IT governance to support cloud computing, cybersecurity, agile methodologies, and cross-functional digital initiatives, all while maintaining strategic alignment and governance flexibility. Recognizing these strategic orientations helps organizations tailor their governance objectives and processes using COBIT 2019's design factor methodology.

### 2.11 Research Framework

To guide this study systematically, a research framework was developed to illustrate the logical sequence of research activities—from problem identification to conclusions and recommendations. The framework ensures that each phase of the research is aligned with the objectives and methodology, while also maintaining consistency with the COBIT 2019 evaluation model.



**Figure 3.** Research Flowchart

As depicted in Figure 3, the research begins with the identification of IT governance issues at Tadulako University, particularly in relation to human resources, infrastructure, organizational structure, and governance processes. After establishing the problem, the next step involves a literature review to explore relevant theories and prior research on IT governance, COBIT frameworks, and capability maturity assessment.

Following this, the data collection phase is carried out using a mixed-methods approach, including interviews, observations, and questionnaires. The data are then processed and analyzed using the Guttman scale to quantify questionnaire results, followed by a capability level analysis in accordance with the COBIT 2019 maturity model. The analysis focuses on the capability of two critical processes: APO12 (Managed Risk) and APO13 (Managed Security). The findings are used to conduct a GAP analysis, comparing the current capability levels with the expected targets. Finally, the framework culminates in the formulation of strategic recommendations aimed at improving IT governance performance at the university.

### **III. Research Methods**

This study employed a mixed-methods approach, combining both qualitative and quantitative methodologies to gain a comprehensive understanding of IT governance at Tadulako University. The qualitative method was used to collect descriptive and subjective data in the form of observations and interviews, which provided rich contextual insights into the current IT governance practices. The quantitative method, on the other hand, was utilized to gather numerical data through questionnaires, which were then analyzed using the Guttman scale and Capability Level Assessment based on the COBIT 2019 framework. This dual approach ensured both depth and objectivity in the research findings.

The research was conducted at Tadulako University, located on Jalan Soekarno Hatta, Palu City, Central Sulawesi, with the postal code 20585. The study took place over a two-month period, from October to November 2022, allowing sufficient time for data collection, analysis, and interpretation. To support the research objectives, both primary and secondary data sources were utilized.

Primary data were obtained through field observations, interviews, and questionnaires. Observations were conducted in a non-participatory manner, with the researcher acting as an independent observer to understand IT operations and organizational behavior. Structured interviews were conducted with three key informants: the Vice Rector for Academic Affairs, the Vice Rector for General Affairs and Finance, and the Head of the ICT Unit (UPT TIK). The interviews explored various themes, including organizational roles and responsibilities, strategic objectives, IT service implementation, technical challenges, and expectations for future governance improvements.

Additionally, questionnaires were distributed to selected respondents within the university's IT environment. The questionnaires were constructed based on the COBIT 2019 framework, particularly its Design Factor model, and focused on two key domains: APO12 (Managed Risk) and APO13 (Managed Security). Each questionnaire included a series of activities corresponding to different capability levels, which were adapted from the COBIT 2019: Governance and Management Objectives guide. The results were analyzed using the Guttman scale to assess compliance levels, and then mapped onto the COBIT 2019 capability maturity scale to determine the current and target governance levels. This methodology ensured that the findings were not only evidence-based but also aligned with global best practices in IT governance.

### **IV. Results and Discussion**

#### **4.1 Identification of Goals Cascade**

This research involves the examination, implementation, and performance measurement of IT governance at the ICT Unit (UPT TIK) of Tadulako University. In this stage, the researcher applies the Goals Cascade model from COBIT 2019, which begins by identifying the Enterprise Goals, followed by the corresponding Alignment Goals, and then the specific Governance and Management Objectives. The Goals Cascade is driven by stakeholder needs and expectations, which are derived from the organization's vision, mission, and strategic objectives. After establishing the enterprise goals, the next step is to determine the governance objectives that are most relevant to the organization using the Design Factors approach in COBIT 2019.

## 4.2 Identification of Enterprise Goals

The initial stage of the analysis involves mapping the vision and mission of UPT TIK Tadulako University to COBIT 2019's standardized Enterprise Goals. This mapping ensures that the goals of the organization align with COBIT's performance dimensions and fall within the Balanced Scorecard (BSC) perspectives: Financial, Customer, Internal, and Growth. The table below presents the identified enterprise goals based on the organization's official mission and strategic functions. Identification of Enterprise Goals

**Table 2.** Enterprise Goal Mapping Based on UPT TIK Tadulako's Vision and Mission

No.	Vision & Mission Statement	Reference (EG)	Enterprise Goal	BSC Perspective
1	Serving as the university's center for data management, documentation, facilities, and information services to support Tridharma and university administration	EG01	Competitive product and service portfolio	Financial
		EG013	Product and business innovation	Growth
2	Preparation of strategic plans, programs, and budgeting	EG06	Business service continuity and availability	Customer
		EG04	Quality of financial information	Financial
3	Development of IT and communication systems	EG06	Business service continuity and availability	Customer
4	IT and communication system management	EG012	Managed digital transformation programs	Growth
5	Provision of ICT services to support academic, research, and community service programs within the university	EG010	Staff skills, motivation, and productivity	Internal

From this mapping, it can be concluded that the organizational goals of UPT TIK align with all four Balanced Scorecard perspectives as defined in COBIT 2019. This demonstrates a comprehensive strategic orientation across financial, customer, internal process, and innovation dimensions.

Reference (EG)	Enterprise Goal
EG01	Competitive product and service portfolio
EG04	Quality of financial information
EG06	Business service continuity and availability
EG010	Staff skills, motivation, and productivity
EG012	Managed digital transformation programs
EG013	Product and business innovation

### 4.3 Identification of Alignment Goals

The second stage in the Goals Cascade process is the identification of Alignment Goals, which serve as a bridge between Enterprise Goals and specific Governance and Management Objectives. These alignment goals are derived by referencing the mapping tables provided in COBIT 2019 (Design Guide – Part 2), where goals marked with “P” (Primary) indicate strong alignment. By identifying which Alignment Goals are linked to each Enterprise Goal, the organization can ensure that its governance processes support its strategic direction. The resulting mapping highlights which alignment goals are most relevant to UPT TIK based on its previously identified enterprise goals. This mapping is critical for defining focus areas and selecting the most appropriate processes to be assessed and improved using the COBIT 2019 framework.

### 4.4 Identification of Governance and Management Objectives

After identifying the relevant Enterprise Goals and their corresponding Alignment Goals, the next stage is to determine the Governance and Management Objectives (GMOs) that are most critical for the organization. This mapping is based on COBIT 2019’s guidance, where each Alignment Goal is linked to specific GMOs through a standard lookup matrix provided in the COBIT 2019 Design Guide (ISACA, 2018).

In this study, the focus was placed on two high-priority objectives relevant to the challenges faced by UPT TIK Tadulako University:

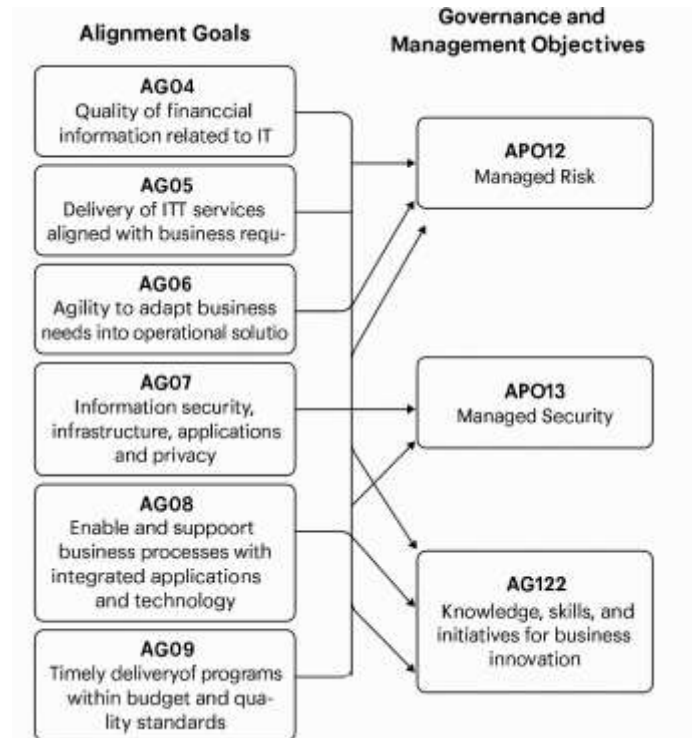
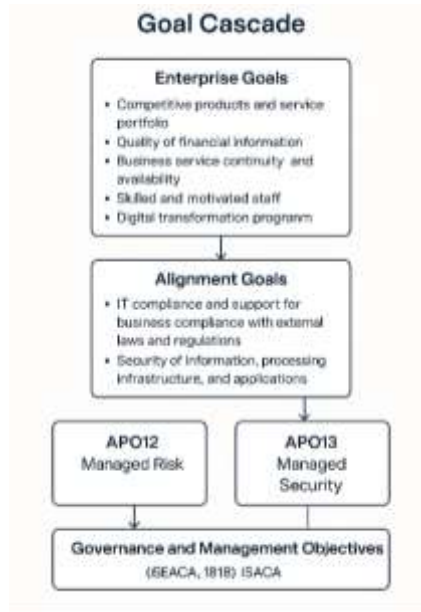
#### a. APO12 – Managed Risk

This objective focuses on identifying, assessing, and mitigating risks that could impact the achievement of enterprise objectives. For UPT TIK, this is essential to address issues such as unstable infrastructure, data integrity, and operational disruptions that may arise due to unmanaged IT-related risks.

#### b. APO13 – Managed Security

This objective ensures that information security is maintained at all levels of the organization. Given that UPT TIK handles sensitive academic and administrative data, strengthening IT security governance is vital to protect against threats and support compliance with national standards and regulations.

These two objectives were selected not only due to their alignment with the organization’s strategy but also based on observed gaps in practice during the preliminary analysis. Both APO12 and APO13 fall under the "Align, Plan and Organize" (APO) domain of COBIT 2019, which deals with high-level planning and strategy management of IT. By focusing on these governance objectives, the study aims to evaluate how well UPT TIK Tadulako is managing risk and security, and to provide concrete recommendations that can help elevate their capability levels in line with international standards.



**Figure 4.** Mapping of Alignment Goals to Governance and Management Objectives

Based on the results of the mapping between Alignment Goals and Governance and Management Objectives, the identified Governance and Management Objectives (GMOs) relevant to UPT TIK Tadulako University can be seen in the table below.



**Table 3.** Mapping Governance and Management Objective UPT TIK UNTAD

Alignment Goals	Governance and Management Objective												
AG 04	APO 06	BAI 09											
AG 05	APO 05	APO 08	APO 09	APO 010	BAI 02	BAI 03	BAI 04	DSS 01	DSS 02	DSS 03	DSS 04	MEA 01	
AG 06	APO 03	APO 04	APO 08	BAI 02	BAI 03	BAI 06	BAI 07	BAI 11					
AG 07	EDM 03	APO 12	APO 13	BAI 10	DSS 04	DSS 05							
AG 08	APO 02	APO 03	BAI 05	DSS 06									
AG 09	EDM 04	APO 06	APO 11	BAI 01	BAI 02	BAI 03	BAI 05	BAI 11					
AG 010	EDM 05	APO 11	APO 14	MEA 01									
AG 012	APO 07	APO 08	BAI 08										
AG 013	APO 04	APO 07	APO 08	BAI 08									

Following the data analysis and identification of key findings related to the current state of information technology within the organization, the process objectives APO12 (Managed Risk) and APO13 (Managed Security) were selected as critical components in supporting the success of the institution's IT-aligned strategic goals. These two objectives reflect the areas most in need of improvement to ensure that IT governance contributes effectively to the broader organizational mission. As a result, this section provides evaluation-based recommendations aimed at improving the organization's IT governance framework. These recommendations are designed to assist the institution in moving from its current capability level (as-is) toward the expected capability level (to-be), as outlined in the COBIT 2019 framework. It is hoped that through the implementation of these targeted improvements, the organization will strengthen its IT management processes and achieve sustainable governance maturity. The following table presents a summary of the key findings and recommended actions derived from the IT governance analysis:

**Table 4.** Assessment Results and Recommendations for IT Governance Objectives (APO12 & APO13)

Governance Objective	Capability Level	Assessment Summary	Recommendations
<b>APO12 – Managed Risk</b>	Level 2	The capability assessment for APO12 (Managed Risk) shows a performance level of 2. According to COBIT 2019, this level indicates that basic activities have been implemented to achieve objectives and are considered to be functioning, though not yet fully optimized. UPT TIK UNTAD has documented several IT risk incidents; however, the process lacks structure and consistency. A more systematic approach is required to ensure IT risk management is aligned with business goals. Despite basic activities being in place, the	UPT TIK UNTAD should develop a formal <b>Project Proposal</b> focused on risk mitigation efforts. This includes preparing <b>IT risk profiles</b> and conducting <b>structured risk governance assessments</b> . Existing risk documentation should be maintained consistently, and <b>periodic evaluations and improvements</b> should be carried out to address recurring incidents effectively.

Governance Objective	Capability Level	Assessment Summary	Recommendations
		process is not operating effectively and does not yet meet the high strategic importance it holds.	
<b>APO13 – Managed Security</b>	Level 1	The capability level for APO13 (Managed Security) was assessed as Level 1. According to COBIT 2019, this level reflects an ad-hoc or intuitive process with limited documentation or formal implementation. Although UPT TIK UNTAD has a designated security unit, it has not been operating effectively in managing, monitoring, and maintaining information security practices. There is no formal documentation on IT security planning and maintenance aligned with organizational goals. This poses a risk to maintaining consistent and secure IT operations.	UPT TIK UNTAD should strengthen the <b>dedicated unit</b> responsible for planning, managing, and monitoring information security. It is recommended to <b>improve documentation</b> related to the design, implementation, and maintenance of <b>security policies and procedures</b> . These efforts should ensure that IT security is properly managed and aligned with the institution's <b>vision and mission</b> .

## V. Conclusion

Based on the analysis conducted, the researcher concluded that the assessment of IT governance capability at the ICT Unit (UPT TIK) of Tadulako University was evaluated using the COBIT 2019 framework, specifically focusing on two governance objectives: APO12 (Managed Risk) and APO13 (Managed Security). The capability levels were measured using performance criteria defined in COBIT 2019, with results summarized in Table 5.

**Table 5.** Summary of IT Governance Audit Results at UPT TIK Tadulako University

Governance Objective	Capability Level Achievement (%)	Actual Level	Target Level	GAP
APO12 – Managed Risk	Level 2: 85% Level 3: 75%	Level 2	Level 4	2
APO13 – Managed Security	Level 1: 82%	Level 1	Level 4	3

As shown in the table above, the capability level for APO12 (Managed Risk) was determined to be at Level 2, with 85% achievement at Level 2 and 75% at Level 3. Although Level 3 was assessed as "Largely Achieved," it did not meet the full

requirements to proceed to the next level. Therefore, APO12 remains at Level 2. This indicates that while risk management practices exist at UPT TIK, they are not yet fully optimized, consistent, or institutionalized, and require further improvement to reach the target level of 4, which represents a state of structured, proactive, and fully integrated governance processes.

For APO13 (Managed Security), the capability was assessed at Level 1, with 82% achievement at Level 2; however, it did not fulfill all the necessary conditions to be considered as fully achieved at that level. As a result, the assessment could not advance to the next stage. This finding implies that while information security practices are present within the organization, they remain basic and inconsistent, lacking the structure and repeatability required for higher maturity.

These results demonstrate a significant gap between the current and expected capability levels, particularly in the area of information security, which holds critical importance in protecting organizational data and ensuring system resilience. Consequently, substantial improvements are needed in both governance objectives to align IT operations with organizational strategy and to ensure effective risk and security management. Recommendations.

Based on the findings of this study, the researcher provides the following recommendations to the organization, with the aim of assisting UPT TIK Tadulako University in achieving its desired capability levels in IT governance: The organization should develop and revise policies related to operational standards across all three core systems under review. Clear and up-to-date policies will serve as a foundation for more consistent and structured governance practices. There is a need for periodic evaluations of IT management processes. Regular monitoring and assessment can help identify gaps, optimize IT functionality, and enhance overall governance performance. It is also recommended that routine IT governance evaluations be institutionalized. This will ensure that capability levels continue to progress in alignment with the organization's strategic goals and that governance maturity can be sustained over time.

For future researchers, it is suggested that subsequent studies applying the COBIT 2019 framework consider conducting a comprehensive assessment of additional governance objectives, beyond APO12 and APO13, to obtain a more holistic understanding of IT governance implementation within UPT TIK at Tadulako University.

## References

- Ahmad, H., Kurniawan, R., & Indrawan, M. (2021). Comparative analysis of IT governance in the public sector using COBIT 5 vs. COBIT 2019. *Jurnal Teknologi dan Sistem Informasi*, 9(2), 231–240.
- Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, 36(6), 907–916. <https://doi.org/10.1016/j.ijinfomgt.2016.05.017>
- Dull, R. B., & Gelinas, U. J. (2008). *Accounting information systems* (8th ed.). South-Western College Pub.
- ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*. ISACA.
- ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- ISACA. (2019). *COBIT 2019 design guide: Designing an information and technology governance solution*. ISACA.

- Komarudin. (1994). Kamus Istilah. Jakarta: Bumi Aksara.
- Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of IT governance on organizational performance. *Journal of Information Systems*, 28(1), 67–81. <https://doi.org/10.2308/isys-50635>
- Nasution, R. A., Siahaan, A. P. U., & Sitorus, S. (2021). Evaluation of information technology governance using COBIT 2019 at a government hospital. *International Journal of Advanced Computer Science and Applications*, 12(6), 498–505.
- Sudjana, N. (2016). Dasar-dasar proses belajar mengajar. Bandung: Sinar Baru Algensindo.
- Swastika, D. (2016). Tata kelola teknologi informasi pada perguruan tinggi. *Jurnal Teknologi Informasi dan Komunikasi*, 4(1), 10–16.
- Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.
- Weill, P., & Vitale, M. R. (2002). What IT infrastructure capabilities are needed to implement e-business models? *MIS Quarterly Executive*, 1(1), 17–34.