Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 25, No. 1, November 2025, pp. 97∼112
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 10/C/C3/DT.05.00/2025
DOI: 10.30812/matrik.v25i1.5628

Developing the Adaptive Digital IT Governance Framework for Next-Generation IT Governance

Bambang Saras Yulistiawan, Rifka Widyastuti, RR Octanty Mulianingtyas, Galih Prakoso Rizky A, Hengki Tamando Sihotang
Universitas Pembangunan Nasional Veteran, Jakarta, Indonesia

Article Info

Article history:

Received August 29, 2025
Revised October 02, 2025
Accepted November 06, 2025

Keywords:

Adaptive IT Governance;
Agile Governance;
Digital Transformation;
Maturity Assessment.

ABSTRACT

The increasing complexity of digital transformation requires an adaptive, measurable, and context-aware IT governance model. However, existing frameworks such as COBIT, ITIL, TOGAF, and ISO/IEC 38500 tend to be partial and prescriptive, failing to address strategic, operational, and innovative needs holistically. This study proposes the Adaptive Digital IT Governance Framework, a novel governance model synthesized from eleven leading IT frameworks and structured into three integrated domains: Govern, Manage, and Adapt. Employing a Design Science Research methodology, the model was developed through a systematic framework analysis, conceptual domain formulation, iterative implementation mapping, and the design of a maturity assessment instrument. The results demonstrate that the Adaptive Digital IT Governance Framework offers a modular, scalable, and value-driven governance solution suited for diverse organizational contexts. Theoretical contributions include extending the IT governance paradigm by integrating strategic alignment, agile governance, and digital sustainability. Practically, the framework provides actionable guidance for designing, assessing, and enhancing digital governance systems across sectors. Unlike previous cross-framework synthesis efforts, the Adaptive Digital IT Governance Framework explicitly introduces the Adapt domain, operationalizing governance agility, innovation capability, and sustainability measurement. This makes the Adaptive Digital IT Governance Framework the first modular, maturity-oriented framework that simultaneously integrates strategy, operations, and adaptability, positioning it as a next-generation model to support organizational resilience and sustainable digital transformation.

Corresponding Author:

Bambang Saras Yulistiawan, +62 816-795-478
Fakultas Ilmu Komputer, Sistem Informasi,
Universitas Pembangunan Nasional Veteran, Jakarta, Indonesia,
Email: bambangsarasyulistiawan@upnvj.ac.id

How to Cite:
B. S. Yulistiawan, R. Widyastuti, R. O. Mulianingtyas, G. P. R. A, and H. T. Sihotang, ”Developing the Adaptive Digital IT Governance Framework for Next-Generation IT Governance”, *MATRIK: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer*, Vol. 25, No. 1, pp. 97-112, November, 2025.

1. INTRODUCTION

Digital Transformation has become a strategic imperative for modern organizations across various sectors, from government to industry. In an era characterized by rapid technological changes, market uncertainty, and constant innovation disruptions, information technology (IT) governance has become increasingly critical. IT governance is not only concerned with risk control and compliance but must also ensure the sustainable creation of business value through adaptive and measurable digital strategies [1–3]. Although various IT governance frameworks, such as COBIT, ITIL, TOGAF, and ISO/IEC 38500, are available, organizations continue to face significant challenges in implementing them comprehensively and in a manner that is contextually aligned with the specific needs of digital transformation.

The root of this problem lies in the fact that these frameworks were developed with differing focal points: COBIT emphasizes control and audit, ITIL focuses on operational services, TOGAF addresses enterprise architecture, and ISO/IEC 38500 outlines general principles of IT governance. This fragmentation often leads organizations to encounter overlaps, domain gaps, or cross-functional integration challenges when attempting to adopt multiple frameworks simultaneously [4]. Furthermore, most frameworks are prescriptive and static, making them less adaptable to the specific needs of organizations undergoing changes driven by digitalization, automation, and heightened efficiency demands.

Previous research has largely focused on implementing a single framework or comparing analyses between frameworks, with relatively few studies attempting to develop a new framework by synthesizing the strengths and weaknesses of multiple existing frameworks. Aversano et al. (2016) highlight that existing governance frameworks are often insufficiently flexible for small and medium-sized enterprises [8]. Meanwhile, Yew et al. (2021) indicate that the effectiveness of frameworks such as COBIT or ITIL is highly dependent on organizational readiness, digital culture, and technology adoption capability factors that are not extensively addressed within the frameworks' own guidelines [5]. In addressing this gap, the present study develops a new IT governance model named ADIGOV (Adaptive Digital IT Governance Framework). This model is designed based on the principles of strategic integration, domain modularity, and sustainability of the implementation cycle. ADIGOV consolidates the core domains of various existing frameworks into a structure comprising three pillars: Govern (strategic direction-setting and control), Manage (service and operational management), and Adapt (innovative capability, agility, and maturity measurement). The design of this framework draws on theoretical foundations from open systems theory [6], the service value cycle model (ITIL v4), and the principles of adaptive digital governance [2]. The objectives of this study are to: (1) systematically identify weaknesses and gaps in eleven leading IT governance frameworks; (2) synthesize relevant and contextually appropriate core components; (3) design a process map and a modular, measurable ADIGOV (Adaptive Digital IT Governance Framework) implementation cycle diagram; and (4) develop a maturity assessment instrument to evaluate the readiness and effectiveness of adopting this framework in real-world organizations.

Accordingly, this research addresses the persistent gap in existing IT governance frameworks, which often lack adaptability, value-orientation, and alignment with the long-term demands of sustainable digital transformation. To respond to this gap, the study contributes in two key ways. Theoretically, ADIGOV enriches the IT governance literature by synthesizing multiple frameworks into a design approach grounded in system adaptivity. Practically, it provides organizations with both a progressive implementation roadmap and a modular maturity measurement tool that are directly applicable and contextually relevant. In doing so, this study lays the groundwork for a governance model that is more responsive, future-oriented, and supportive of sustainable digital transformation while also clarifying how ADIGOV advances beyond prior integration or harmonization efforts. Despite several prior attempts to combine or harmonize IT governance frameworks such as COBIT, ITIL integrations, enterprise-architecture centric governance models, and hybrid approaches using ISO/IEC standards, these efforts often remain either overly conceptual or narrowly scoped to specific domains (for example, service management or compliance) and therefore fail to deliver a holistic, operationally actionable solution for digital-era organizations. Empirical and review studies show frequent emphasis on control, service operations, or architecture in isolation, with limited treatment of iterative maturity progression and adaptive governance mechanisms required for VUCA environments [7]. Moreover, the growing literature on agile/adaptive governance highlights organizational agility, cross-functional decision layers, and governance-for-innovation as emergent priority areas insufficiently integrated into classical frameworks or prior synthesis efforts [8, 9]. Crucially, many earlier synthesis proposals lack a clear, modular maturity mechanism that enables organizations to iteratively evolve governance capabilities (from strategic alignment to service execution to innovation governance) in response to changing business and technology contexts. This lacuna justifies a modular, measurement-oriented synthesis like ADIGOV that explicitly introduces an Adapt domain to support governance flexibility, digital resilience, and sustainable innovation, thereby offering both theoretical grounding and practical implementability for organizations navigating rapid digital transformation [10].

2. RESEARCH METHOD

The development of the ADIGOV (Adaptive Digital IT Governance Framework) model is grounded in the Design Science Research (DSR) methodological approach [11], which emphasizes the creation and evaluation of innovative solutions to address

real-world problems, particularly in the context of adaptive information technology governance in the digital era. The model's development process was carried out in an iterative and structured manner, encompassing three major phases: analysis of existing frameworks, formulation of core domains and processes, and visualization of the model's architecture, as depicted in the ADIGOV Process Map.

The initial stage began with a systematic analysis of eleven major IT frameworks, namely COBIT 5 & 2019, ITIL v4, TOGAF, ISO/IEC 38500, ISO/IEC 20000, PMBOK, CMMI, DevOps, SAFe, IT4IT, and the Zachman Framework. Through a framework comparative analysis process, the strengths and weaknesses of each framework were mapped against seven evaluation dimensions: domain completeness, adaptability, service value cycle, data governance and security, innovation and agility, application of ethics and sustainability, and cross-sector applicability. This study is further supported by a literature review of more than 70 Scopus and Web of Science-indexed articles evaluating the effectiveness of these frameworks in the context of digitalization across public and private sectors [12].

The analysis revealed that none of the existing frameworks fully meet the requirements of adaptive and dynamic digital governance. COBIT 2019 excels in governance structure but falls short in innovation and digital resilience. In contrast, ITIL and DevOps demonstrate strengths in service management but insufficiently address strategic and sustainability dimensions. This led to the identification of a research gap: the need for a new framework that integrates strategic, operational, and adaptive dimensions to respond to the evolving complexities of modern digital organizations effectively.

The research design was carried out in five main stages. The first stage was problem identification and motivation, involving a systematic analysis of the weaknesses of eleven major IT frameworks (COBIT, ITIL, TOGAF, ISO/IEC 38500, ISO/IEC 20000, CMMI, PMBOK, DevOps, SAFe, IT4IT, and the Zachman Framework). This analysis was conducted through a review of relevant academic and practical literature, as well as an examination of official documentation from each framework. The second stage was defining the objectives for a solution, specifically formulating the objectives for developing the ADIGOV framework based on the gaps and unmet needs of modern digital organizations that existing frameworks have yet to address.

The third stage was design and development, in which the researchers structured the ADIGOV model into three main domains: Govern, Manage, and Adapt, each consisting of subdomains and core processes. At this stage, a process map and an implementation cycle diagram (ADIGOV Cycle) were designed to demonstrate the logical and iterative flow of the framework application. Additionally, a maturity assessment instrument (ADIGOV Maturity Assessment Tool) was developed, based on five levels (Initial, Repeatable, Defined, Managed, Optimized), to assist organizations in evaluating their readiness and the effectiveness of framework adoption. The fourth stage was initial validation through contextual adaptation. The fifth stage was visual design and mapping tools for maturity measurement. The following diagram (Figure 1) illustrates the Research Methodology Flow for the Development of the ADIGOV Framework.

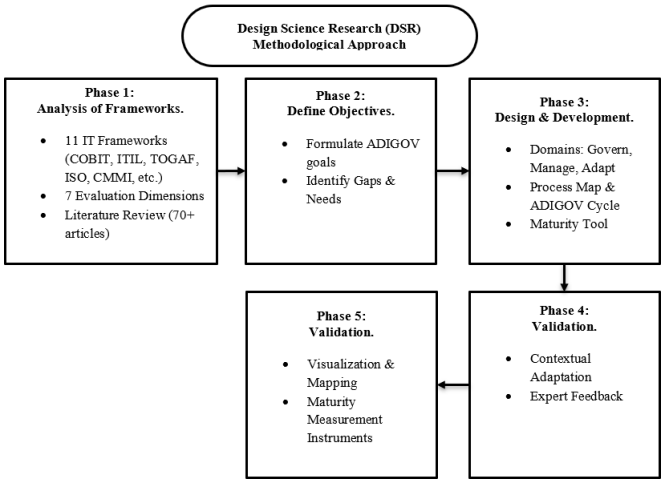

Figure 1. Research Methodology Flow for ADIGOV Framework Developmen

2.1. Model Validation and Limitations

The research process was carried out in five main stages: (1) Framework Analysis systematically reviewing and comparing eleven existing IT governance frameworks (COBIT, ITIL, TOGAF, ISO/IEC 38500, etc.) to identify their strengths and limitations;

(2) Domain Formulation synthesizing core governance components and clustering them into three main domains (Govern, Manage, Adapt); (3) Framework Design constructing the ADIGOV process map and modular implementation cycle; (4) Conceptual Validation conducting expert reviews and limited workshops to verify theoretical soundness and completeness; and (5) Maturity Tool Mapping developing a measurement instrument to evaluate organizational readiness and iterative improvement. Validation in this study primarily relies on conceptual testing through expert panels and limited case studies involving selected organizations. While this provides an initial level of confidence in ADIGOV's relevance and applicability, it does not yet constitute a full-scale empirical or quantitative evaluation across multiple sectors or organizational maturity levels. Consequently, the current results are a proof-of-concept that demonstrates the feasibility and theoretical robustness of the framework, but they are not yet generalizable empirical evidence. Future research is recommended to conduct broader surveys, multi-organization pilots, and statistical analyses (e.g., structural equation modeling) to quantitatively assess ADIGOV's impact on IT governance performance, agility, and value creation [13].

2.2. Weakness Analysis

The Development of the ADIGOV (Adaptive Digital Governance Framework) model began with an in-depth analysis of eleven dominant information technology governance frameworks in practice, namely COBIT 5 & 2019, ITIL v4, TOGAF, ISO/IEC 38500, ISO/IEC 20000, PMBOK, CMMI, DevOps, SAFe, IT4IT, and the Zachman Framework. This review employed a comparative framework analysis approach to identify areas of strength, weakness, and implementation gaps in each framework. Several key findings from this study are as follows: COBIT 5 and COBIT 2019 excel in governance structure and value measurement but are less responsive to disruptive technological change and less supportive of innovation and digital resilience contexts (De Haes & Van Grembergen, 2015; ISACA, 2019). ITIL v4 offers comprehensive coverage of service management; however, it is overly focused on operations and includes limited strategic or innovative domains. TOGAF excels in enterprise architecture; however, it is overly heavy and complex for non-IT organizations and demonstrates weaknesses in adaptive dimensions. ISO/IEC 38500 contains elegant governance-level principles but remains high-level in nature, thereby requiring complementary operational frameworks. ISO/IEC 20000 and PMBOK focus solely on service and project aspects, with limited capacity to support comprehensive governance. DevOps and SAFe are effective for agile delivery but are not designed for sustainable governance and risk control. IT4IT is highly technical and well-suited for managing IT value streams; however, it has limited applicability within public organizations and governance models. The Zachman Framework is descriptive in nature and provides limited concrete guidance for adaptive digital governance. These findings are reinforced by a systematic review of over 70 scholarly publications from reputable journals (Q1/Q2) that evaluate the implementation of these frameworks in both government and industry sectors. Many studies emphasize the importance of integrating strategic governance, service management, digital innovation, organizational resilience, and the principles of ethics and sustainability [12].

2.3. Phase of the New Model Development

The development of the Adaptive Digital IT Governance (ADIGOV) framework was carried out through a structured, multi-phase process to ensure methodological rigor and comprehensive coverage. Each phase was designed to build upon the preceding stage, allowing for systematic identification, evaluation, and integration of key governance elements into a coherent framework. The following subsections describe the sequential phases undertaken in the model development process.

Phase one: Analysis of Weaknesses and Overlaps in Existing Frameworks, The initial step in developing ADIGOV began with a meta-framework study of eleven globally recognized frameworks commonly applied in information technology governance and management, namely COBIT 5 & 2019, ITIL v4, TOGAF, ISO/IEC 38500, ISO/IEC 20000, PMBOK, CMMI, DevOps, SAFe, IT4IT, and ISO/IEC 27001. This analysis was conducted systematically using domain function mapping and a capability overlap matrix approach to identify areas that are redundant, insufficiently integrated, or overlapping.

The findings reveal that most frameworks predominantly emphasize either the governance or the management dimension, without sufficiently integrating organizational adaptability and innovation capabilities. For instance, ISO/IEC 38500 is overly normative and lacks operational applicability, whereas DevOps and SAFe place strong emphasis on technical execution and development speed but demonstrate weaknesses in governance principles [14, 15]. This underscores the need for a framework that unifies strategic governance principles, service management, and adaptive digital resilience.

The following section provides a detailed account of the limitations of eleven globally recognized information technology (IT) frameworks, which form the primary foundation for developing the ADIGOV model. As summarized in Table 1 (State of the Art) below, this analysis draws upon scholarly literature, systematic reviews, and implementation reports from both public and private sectors. Highlighting these limitations is essential, as it not only reveals the structural and operational gaps within existing frameworks but also establishes the rationale for proposing ADIGOV as a more adaptive, integrated, and context-responsive governance model.

Table 1. State of The Art

Framework	Researcher	Limitation
COBIT 5 & COBIT 2019	Lopes & da Silva, 2021,	Implementation Complexity: COBIT is known for its complex structure, making full adoption challenging, particularly for organizations with limited IT resources.
	De Haes et al, 2020 [4]	Strong governance focus, limited support for innovation: while robust in governance structure, COBIT demonstrated limited flexibility in the context of digital innovation and organizational resilience to disruption.
	Al Omari, Loai (2016) [16]	Lack of contextual adaptability: COBIT is not sufficiently adaptive to the specific contexts of sectors or countries and does not explicitly accommodate governance agility.
	Galup et al., 2009 [17]	Overemphasis on Service Operationalization: ITIL v4 is highly effective in service management but demonstrates weaknesses in supporting long-term business strategies and holistic organizational governance.
ITIL v4	Axelos, 2020 [18]	Limited Adaptability to Digital Ecosystems and Emerging Business Models: ITIL does not fully capture the dynamics of cloud-native environments, DevOps practices, or platform-based digital business models.
	Iden & Eikebrokk, 2014 [19]	Lack of Explicit Support for Innovation and Agility: ITIL is predominantly procedural in nature and does not yet provide comprehensive support for the agility of digital organizations.
	Lankhorst, 2017	Excessive Abstraction: TOGAF is often criticized for being overly theoretical and providing limited operational guidance for implementation.
TOGAF (The Open Group Architecture Framework)	Kurniawan et al., 2022	Limited Agility in Responding to Rapid Business Changes: TOGAF does not explicitly support governance agility or digital innovation in volatile, uncertain, complex, and ambiguous (VUCA) environments
	Judijanto, Loso, et al, 2023	Lack of Integration with Current Security and Innovation Practices: Primarily focuses on technical and business architecture, without comprehensively addressing cybersecurity risks and digital ethics
	Selig, G. (2008) [20]	Overly Normative and Generic: This standard provides only the fundamental principles of IT governance and lacks detailed implementation guidance.
ISO/IEC 38500	Peterson, 2004	Does Not Support Digital Transformation: Fails to accommodate dimensions of agility, digital innovation, or sustainability in modern IT transformation.
	De Haes & Van Grembergen, 2009	Lack of Performance and Maturity Measurement: Does not provide indicators for capability assessment or IT governance performance evaluation.
	Schenk, B. (2025)	Overemphasis on Traditional IT Service Management: Insufficiently adaptive to cloud technologies, DevOps practices, and platform-based digital services.
ISO/IEC 20000	Ali	Green, 2007 [**?**] & Lack of Integration with Strategic Governance: Does not accommodate strategic decision-making within IT governance.
	Pollard & Cater-Steel, 2009	Certification Does Not Always Enhance Business Value: Implementation of ISO/IEC 20000 often becomes a formality and does not necessarily result in significant improvements in organizational capabilities.
	Serrador & Pinto, 2015	Misalignment with Agile Practices: PMBOK is highly formal, bureaucratic, and slow to apply in digital or innovative projects.
PMBOK (Project Management Body of Knowledge)	Kerzner, 2017 [21]	Overly Narrow Focus on Project Management: Does not support IT governance, innovation, or organizational sustainability aspects.
	Turner & Müller, 2003	Limited Suitability for Day-to-Day Operational Execution: Not relevant for organizations with iterative processes and continuous product delivery.
	Paulk, 2009 [22]	Overemphasis on Formal Processes: Provides limited support for innovation, flexibility, and process adaptation in dynamic environments

(continued on next page)

Table 1 (continued)

Framework	Researcher	Limitation
CMMI (Capability Maturity Model Integration)	de Ataíde Ramos, V. S. S. (2014) [23]	Difficult to Apply in Non-Technical Organizations: CMMI is more suitable for software development organizations and less applicable to public service or hybrid institutions.
	Staples & Niazi, 2008	Heavy implementation and high cost: known for being costly and requiring highly skilled human resources for implementation
	Wiedemann, A. (2018) [24]	Focus on Technical Aspects Rather Than Governance: DevOps places strong emphasis on collaboration between developers and operations teams but is weak in governance, compliance, and strategic value
DevOps	Buschow, C. (2020)	Not Suitable for All Organizations: Highly effective in startups or digital-native companies but not always relevant in the public sector or large organizations with strict regulatory requirements.
	Proenca, D., & Borbinha, J. (2018)	Lack of Maturity Structure: does not provide a formal maturity model that can be used as an assessment tools.
	Knaster	Leffingwell, 2020 [25] & High complexity at large scale: although termed ”scaled” SAFe can be highly complex and bureaucratic in practical implementation
SAFe (Scaled Agile Framework)	Mergel, I. (2016)	Overly Narrow Focus on Agile Delivery: Does not provide a comprehensive framework for governance and compliance.
	Kurucz, et al., 2017	Limited Support for Sustainable Strategy and Governance: Does not explicitly address sustainability, ethics, or strategic capabilities.
	Tervajoki, Mikko, 2017 [26]	Overemphasis on Tool-Centric Processes: IT4IT is primarily used to align tool-based processes rather than integrate strategic value.
IT4IT	The Open Group, 2017	Limited Testing Across Multiple Sectors: IT4IT is relatively new and has not been widely implemented in public sector or governmental organizations.
	Maleh, Y., & Sahid, A. (2024) [27]	Lack of Coverage for Innovation, Resilience, and Ethical Governance: IT4IT has yet to accommodate dimensions of soft governance and resilience.
	Veiga, A. D et al., 2011	Focus Solely on Information Security: Does not address IT governance, innovation, or capability management aspects.
ISO/IEC 27001	Leupold et al., 2007	Insufficient Adaptability to Cloud and DevOps Innovations: Too rigid in handling modern risks such as shadow IT or CI/CD pipelines.
	Siponen & Willison, 2009	Does Not Drive Strategic Business Value: The standard is more protective than enabling.

Based on these conceptual gaps, the design process of the ADIGOV model was carried out using the Design Science Research (DSR) approach, which consists of the following stages: problem identification, objective definition, design & development, demonstration, and evaluation.

Phase two: Structuring Domains and Dimensions Based on Literature Grounding. Based on the previous analysis, three main domains were established: Govern, Manage, and Adapt. Each domain is grounded in well-established theories and concepts: The GOVERN domain is grounded in the theory of strategic alignment, value realization [1], and risk and compliance principles based on enterprise risk management. It focuses on addressing the strategic and value aspects of a digital organization, comprising the processes of Strategic Alignment, Value Realization, and Risk & Compliance. This domain adapts principles from COBIT, ISO/IEC 38500, and value-based governance [1]. The MANAGE domain is developed based on the ITIL, ISO/IEC 20000, and PMBOK frameworks, reinforced by the theories of service lifecycle (OGC, 2011), information security management (ISO/IEC 27001), and capability maturity [28]. It encompasses the operational management of services and information security through three main processes: Service Lifecycle Management, Information Security, and Performance & Capability Management. This domain synthesizes elements from ITIL v4, DevOps, ISO/IEC 27001, and CMMI. The ADAPT domain is introduced as a response to the need for digital resilience and agility in the VUCA era. It adopts concepts from agile governance [29], innovation capability, governance flexibility, as well as digital sustainability and ethics. It represents the adaptive capacity and long-term sustainability of an organization through three processes: Innovation & Agility, Governance Flexibility, and Sustainability & Ethics. This domain addresses the gaps in traditional frameworks in supporting VUCA dynamics and digital ethics. The ADIGOV model is developed in a modular manner and can be implemented progressively according to the organization's maturity level. Each domain is equipped with guiding principles, a metric structure, and performance indicators that can be measured through a maturity assessment. Furthermore, the model supports extension to both

public and private sectors and can be tailored for institutions of various scales.

Phase Three: Integration of Maturity, Agility, and Sustainability Elements into the Model. Each domain is broken down into three subdomains/functions, organized sequentially from the strategic, tactical, to executional level. The objective is to align the hierarchical structure of organizational responsibilities with the stages of achieving digital capabilities (Weill & Woerner, 2018). This model also introduces the principles of agile governance and adaptability, two aspects that have been largely underrepresented in traditional frameworks. For the ADAPT domain in particular, emphasis is placed on governance flexibility and digital ethics to address regulatory pressures, public expectations, and risks inherent in the digital ecosystem [30].

Phase Four: Initial Validation through Contextual Adaptation. After the domain and subdomain framework was established, the ADIGOV model was conceptually validated through case studies in several government organizations and public institutions that adopted multiple IT frameworks. This approach employed the Design Science Research (DSR) methodology in three stages: relevance cycle, design cycle, and rigor cycle [31]. The results demonstrated that dividing into three domains facilitated more adaptive and context-sensitive mapping of roles, maturity assessments, and governance reporting.

Phase Five: Visual Design and Mapping Tools for Maturity Measurement. The final phase is to develop a visual process map, as illustrated in the image you provided. Each domain consists of three main components: GOVERN, which consists of Strategic Alignment $\longrightarrow$ Value Realization $\longrightarrow$ Risk & Compliance. MANAGE covers Service Lifecycle $\longrightarrow$ Information Security $\longrightarrow$ Performance & Capability. ADAPT includes Innovation & Agility $\longrightarrow$ Governance Flexibility $\longrightarrow$ Sustainability & Ethics. This structure is designed to support domain-based maturity assessments and to facilitate the development of modular maturity assessment tools.

2.4. The ADIGOV model has been structured into three main domains, as visualized in Figure 1 (The ADIGOV Process Map).

As a result of the in-depth analysis and synthesis conducted, the ADIGOV model has been formulated into three interconnected main domains. These domains form a comprehensive framework to support governance, risk mitigation, and adaptive innovation development within a digital context. This structure is clearly visualized in Figure 1 below, which illustrates the flow and interrelations among the domains in the ADIGOV Process Map.

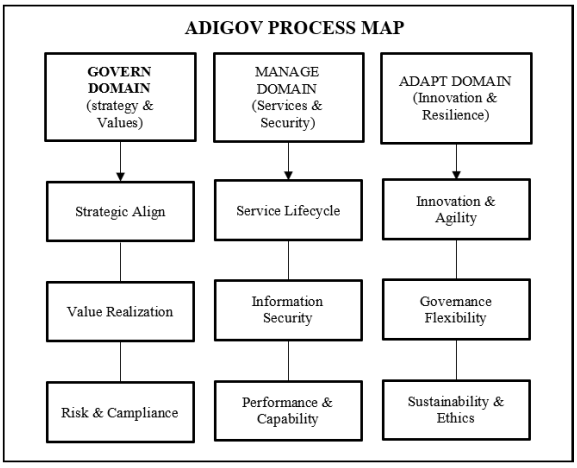

Figure 2. The ADIGOV Model

The ADIGOV model is conceptually designed around three main domains: GOVERN, MANAGE, and ADAPT as an integrated framework to address the need for more relevant, flexible, and digitally sustainable information technology governance (Figure 2). This structure emerged from a critical synthesis of the fragmentation and functional overlaps found in eleven global frameworks, supported by scholarly literature and empirical studies that emphasize the importance of integrating strategy, operations, and innovation.

First, the GOVERN domain is designed to address organizational needs in setting strategic direction, ensuring alignment between IT and business objectives, and managing risk and compliance. Frameworks such as ISO/IEC 38500 emphasize governance principles but are often overly normative and lack operational guidancev, while COBIT provides detailed controls but still requires

high-level interpretation within a strategic context [32, 33]. GOVERN fills this gap by integrating the principles of strategic alignment, value realization, and enterprise risk management.

Second, the MANAGE domain adopts the operational management dimension encompassing service lifecycle, information security, and performance capability. Frameworks such as ITIL, DevOps, and ISO/IEC 20000 focus on IT service efficiency and operations but tend to have limited coverage of strategic governance. Additionally, frameworks like CMMI and PMBOK emphasize managerial processes but are less connected to value and risk cycles. This domain synthesizes principles of Service Lifecycle Management [34], Information Security Governance (ISO/IEC 27001), and performance-based capability management.

Third, the ADAPT domain represents ADIGOV's key differentiator, encompassing digital resilience, organizational innovation, and governance flexibility that are critical in the VUCA (volatility, uncertainty, complexity, ambiguity) era. Traditional frameworks such as TOGAF, SAFe, and IT4IT have yet to explicitly establish adaptability as a distinct domain, despite its growing importance in the context of digital transformation. ADAPT draws upon recent literature related to Digital Transformation Capability, Agile Governance, and Digital Sustainability to ensure organizations can innovate sustainably while maintaining ethical standards and social responsibility.

This three-domain structure is not only a conceptual representation but also facilitates the implementation of the model, organizational maturity measurement, and the development of modular, interoperable tools. Through this approach, ADIGOV addresses the current demands of IT governance in a holistic, adaptive, and measurable way.

3. RESULT AND ANALYSIS

From the results of the development of the new model (ADIGOV: Adaptive Digital IT Governance Framework) presented in the previous section, this section will elaborate on how the new model provides an integrative IT governance and management approach, based on value, risk, and service, while being adaptive to organizational scale and the needs of modern digital business.

3.1. The Result of the ADIGOV Model Development (Adaptive Digital IT Governance Framework)

This research resulted in a new IT governance framework called ADIGOV (Adaptive Digital IT Governance Framework). The model is designed to integrate the strengths of various existing frameworks while addressing gaps that conventional approaches have not accommodated. The ADIGOV model consists of three main domains: (1) Govern Domain, (2) Manage Domain, and (3) Adapt Domain. Each domain is further detailed into three core processes, as illustrated in Figure 1.

The Govern Domain focuses on strategic alignment, value realization, and risk and compliance management. The Manage Domain addresses the service lifecycle, information security, and performance & capability aspects. Meanwhile, the Adapt Domain is introduced as the key innovation within ADIGOV, encompassing processes of innovation & agility, governance flexibility, and sustainability & ethics.

The development of ADIGOV was conducted using a design science research (DSR) approach, involving the construction of the model based on a systematic literature review, thematic synthesis of 11 major frameworks (including COBIT, ITIL, TOGAF, ISO 38500, ISO 27001, etc.), and substantial validation through expert analysis and the needs of public sector organizations. Thus, this model is not only conceptual but also grounded in practical and contextual requirements.

To support effective implementation, ADIGOV is designed with a set of fundamental principles that serve as both philosophical and practical foundations. These principles ensure that the ADIGOV model can be applied adaptively, relevantly, and sustainably across various organizations with differing needs and complexities. The core principles of ADIGOV emphasize a value-driven approach focusing on creating and realizing value from IT, a risk-informed perspective that integrates risk management as the basis for decision-making, and a service-integrated orientation that, like ITIL, extends to the governance level. The model is agile and scalable, making it suitable for organizations of all sizes through its modular approach. It is security-aware by integrating security from the design phase through to operations, stakeholder-engaged by involving business, regulators, and IT stakeholders, and continuously measured with performance and maturity evaluated both quantitatively and qualitatively.

The structure of the ADIGOV Framework. To establish holistic and adaptive governance, the ADIGOV framework is structured around three core domains: Govern, Manage, and Adapt. Each domain encompasses a set of subdomains that address strategic, operational, and responsive dimensions, ensuring alignment with the dynamic nature of the digital environment. This structural design not only provides a clear roadmap for implementation but also offers the necessary flexibility for organizations to tailor their governance approach to their specific needs, organizational scale, and internal capabilities. To illustrate this foundation in greater detail, Table 2 (The Structure of ADIGOV) below presents a comprehensive overview of the framework, outlining its core domains, subdomains, and the primary focus areas within each, thereby serving as a structured guide for both analysis and application:

Table 2. The Structure of ADIGOV

Domain	Subdomain	Focus
Govern	Strategic Alignment	To align the IT strategy with the business objectives
	Digital Value Realization	To ensure business value realization from IT investments
	Risk & Compliance Oversight	Oversight of digital risk and compliance
Manage	Digital Service Lifecycle	Planning, delivery, and improvement of IT services
	Information Security & Resilience	Integration of information security and resilience
	Performance & Capability	Measurement of IT performance and human resource capabilities
Adapt	Governance Flexibility Layer	Modularity is adaptable to organizational scale
	Innovation & Agility	Responsiveness to disruption and digital transformation
	Sustainability & Ethics	Sustainable and ethical IT governance

With this thematically organized structure, ADIGOV provides comprehensive guidance for organizations to manage information technology strategically and sustainably. Each element within the framework is designed to complement one another, forming a governance system that is modular, flexible, and ready to address the challenges of digital transformation across diverse sectors. GOVERN Domain, The GOVERN domain in ADIGOV serves as the strategic foundation that ensures the direction and objectives of information technology (IT) are aligned with the organization's business vision. This domain emphasizes the importance of value creation, risk management, and regulatory compliance as integral components of digital governance. Each subdomain within GOVERN is designed to address the organization's strategic challenges and provide tools for data-driven planning and decision-making. As shown in Table 3 (The GOVERN Domain in ADIGOV) below, these subdomains are outlined together with their key activities and expected outputs:

Table 3. The GOVERN Domain in ADIGOV

Subdomain	Main Activity	Output	Assessment Indicator
Strategic Alignment	To align the IT strategy with the business objectives	IT Strategy Map	Management involvement, IT strategy map, IT-business KPI alignment
Value Realization	Evaluation and monitoring of IT value	Digital Value Dashboard	Evaluation of IT value, benefit tracking, and value-based decisions
Risk & Compliance Oversight	Risk identification and regulation mapping	Risk register and compliance report	IT risk mapping, compliance report, internal control

With a structured approach within the GOVERN domain, organizations can ensure that IT investments not only contribute to achieving business objectives but also remain compliant, are managed securely, and deliver tangible value. The three core subdomains, Strategic Alignment, Value Realization, and Risk & Compliance Oversight, serve as key pillars in establishing a digital governance framework that is well-directed, measurable, and trustworthy. MANAGE Domain, The MANAGE domain in ADIGOV focuses on the comprehensive operational management of information technology. This domain encompasses the management of the digital service lifecycle, information security and resilience, as well as the evaluation of performance and human resource capabilities. Its objective is to ensure that IT services not only operate effectively but are also secure, resilient, and capable of delivering measurable added value. As summarized in Table 4 (The MANAGE Domain in ADIGOV) below, the subdomains of the MANAGE domain are detailed along with their key activities and resulting outputs.

Table 4. The MANAGE Domain in ADIGOV

Subdomain	Main Activity	Output	Assessment Indicator
Service Lifecycle	End-to-end service management	SLA/OLA, service catalog	Service procedure, SLA/OLA, service catalog
Information Security & Resilience	Security, backup, recovery, and disaster	ISMS, disaster recovery plan	ISMS, BCP/DRP, awareness training
Performance & Capability	IT and HR KPI assessment	KPI report, competency Matrix	Dashboard of KPI IT, HR development, and competency analysis

Through the MANAGE domain, ADIGOV provides a concrete and measurable operational framework for organizations. Subdomains such as Service Lifecycle, Information Security & Resilience, and Performance & Capability play a crucial role in ensuring

that every digital service is not only functional but also meets high standards of security, performance, and human resource competence. In this way, MANAGE serves as the backbone of operational sustainability within digital governance.

The ADAPT Domain in ADIGOV is designed to ensure that digital governance can continuously evolve and adjust to technological dynamics, organizational needs, and stakeholder expectations. The primary focus of this domain lies in flexibility, innovation, sustainability, and ethics in IT management. ADAPT enables organizations to design modular structures, respond to change through agile approaches, and uphold social and ethical responsibility in every digital aspect. The following table outlines the ADAPT subdomains along with their key activities and expected outputs (Table 5).

Table 5. The ADAPT Domain in ADIGOV

Subdomain	Main Activity	Output	Assessment Indicator
Governance Flexibility	Process and Control Modularization	Implementation modular model	Modular documentation, adaptive SOPs, risk-based approach
Innovation & Agility	Integrated Innovation & agile governance	Innovation Project, Sprint Review	Innovation project, Sprint Review, pilot test
Sustainability & Ethics	Sustainable and ethical governance	Digital code of ethics, Ethics audit	Digital code of ethics, Ethics audit, green IT initiative

As shown in Table 5 (The ADAPT Domain in ADIGOV), adopting these principles enables organizations not only to respond effectively to digital disruptions but also to establish governance that is innovative, sustainable, and ethical. The three core subdomains Governance Flexibility, Innovation & Agility, and Sustainability & Ethics serve as the driving forces for a governance model that is both responsive and responsible, ensuring that ADIGOV remains relevant over the long term.

One of the key strengths of ADIGOV lies in its dynamic and continuous cyclical approach. This model adopts an iterative principle to ensure that digital governance is not static but continually evolves in line with organizational needs and external changes. The ADIGOV cycle consists of five interrelated stages that form a recurring loop, driving continuous improvement. As illustrated in Figure 3 (The ADIGOV Cycle), each stage is explained in detail below.

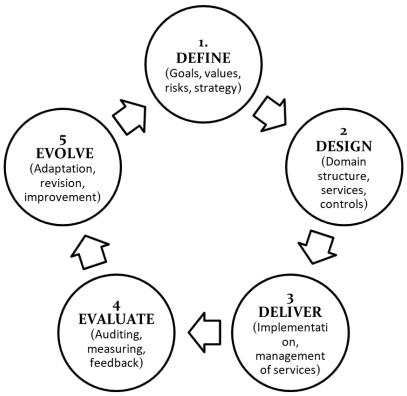

Figure 3. The ADIGOV Cycle

Table 6. The DescriptionADIGOV Cycle

Phase	Main Activity	Output
Define	Arranging the vision, principle, and IT strategy map	Strategic Plan, Risk Map
Design	Designing process, controls, SLAs, and roles	Process Architecture, SOP, RACI
Deliver	Managing services, human resources, security, and operations	Service operations and performance reporting
Evaluate	Conducting monitoring, internal audits, and user surveys	Dashboard KPI, risk evaluation
Evolve	Iteration processes, fostering learning, and driving innovation	Improvement planning and new technology adoption

Through the five stages presented in Table 6, ADIGOV provides a structured yet flexible approach that enables organizations to navigate the complexities of digital transformation in a measured, responsive, and value-oriented manner. This cycle serves as the foundation for establishing digital governance that is sustainable and adaptive to contemporary challenges. Performance indicators

and Maturity Assessment, To ensure that the implementation of ADIGOV is both effective and measurable, a comprehensive evaluation system is required through Key Performance Indicators (KPIs) and maturity assessments. Each area of digital governance, ranging from services and security to strategy, has its own specific metrics and assessment tools. This approach enables organizations to monitor performance both quantitatively and qualitatively, while also identifying areas in need of improvement.

Table 7. Performance Indicators and Maturity Assessment

Area	Main KPI	Assessment Tool
Service	Response time, user satisfaction	Service survey, ITSM Reports
Security	Number of incidents, recovery time	Dashboard ISMS
Strategy	ROI IT, business alignment	Value Scorecard
Maturity process	Level 1–5	ADIGOV Maturity Tool (berbasis CMMI+COBIT)

As presented in Table 7, through monitoring performance indicators and measuring maturity levels, ADIGOV enables organizations to evolve systematically. This evaluation is not merely administrative; it serves as the foundation for more accurate, strategic, and continuous improvement–oriented decision-making. Thus, the digital governance process does not end at planning and implementation but is continuously refined through measurement and learning.

To assess the effectiveness of digital governance implementation within an organization, ADIGOV adopts a maturity scale derived from a combined approach of the Capability Maturity Model Integration (CMMI) and COBIT Maturity Levels. This scale provides an overview of process readiness and control, ranging from the most basic condition to a highly adaptive and sustainable stage. Such assessments help organizations identify their current position and develop targeted improvement strategies. The following outlines the maturity levels used in the ADIGOV model.

Table 8. Maturitas Level Proses (Berbasis CMMI + COBIT)

Level	Name	Description
0	Non-Existent	There is no process or awareness
1	Initial / Ad Hoc	It is undocumented and highly reactive
2	Repeatable	Basic practices are in place
3	Defined	The process is documented and training
4	Managed	Monitoring process and metrics-based

As shown in Table 8, this maturity scale allows organizations to evaluate not only the existence of processes but also their quality, consistency, and adaptability to change. By identifying their position between levels 0 and 5, organizations gain an objective foundation for continuous improvement while mapping a more mature and structured digital transformation roadmap. Once the maturity assessment is conducted for each area of digital governance, the obtained scores can be averaged to provide an overall picture of the organization's position. Interpreting this total score is crucial for decision-makers to understand the readiness and quality of the current governance. Using an easy-to-read color categorization system, the following table presents the classification of average scores along with their implications for the next development strategy:

Table 9. Total Score Interpretation

Average score	Category	Implication
0–1.5	Red (Critical)	Governance is not effective, with a priority on building basic development
1.6–2.9	Yellow (Developing)	Initial processes need formalization and strengthening
3.0–3.9	Light Green (Managed)	Fairly good governance requires performance improvement
4.0–5.0	Dark Green (Leading)	Already excellent, focus on innovation and optimization

As presented in Table 9, the interpretation of the total score serves not only as a reflection tool but also as a strategic compass for determining the most relevant improvement actions. A higher score indicates a more mature and adaptive digital governance system, while a lower score signals the need for structural interventions to strengthen governance foundations. Thus, this evaluation becomes an integral part of the continuous improvement cycle within the ADIGOV framework.

Implementation and Improvement Plan: To ensure that the ADIGOV model can be implemented effectively and deliver tangible impact for organizations, a systematic and sustainable implementation plan is essential. This plan covers stages from initial preparation to continuous improvement based on evaluation and feedback. Each stage has specific key activities and outputs, serving

as a guide for organizations to adopt the ADIGOV framework in a gradual yet well-directed manner. Below are the implementation and improvement stages of ADIGOV, along with the key activities and expected outcomes.

Table 10. Implementation and Improvement Plan

Stages	Activity	Output
Preparation	Readiness analysis, training	Gap Analysis Report
Implementation	Pilot of priority domains	Phase 1 ADIGOV project
Evaluation	Internal audit	Compliance report
Improvement	Revision based on feedback	Advanced version of the framework

As shown in Table 10 (Implementation and Improvement Plan), following these stages enables organizations to build a strong foundation for implementation. It also allows organizations to implement ADIGOV in a controlled manner through pilot projects. Furthermore, periodic evaluations and feedback-driven improvements become crucial steps to maintain the framework's relevance and ensure its alignment with the evolving demands and challenges of the digital landscape.

3.2. Discussion

The findings of this study indicate that ADIGOV successfully addresses various shortcomings found in previous frameworks in a direct manner, both in terms of integration, functional completeness, and adaptability to the digital environment. First, in terms of domain integration. Frameworks such as COBIT and ISO/IEC 38500 emphasize strategic governance but are weak in operationalizing services. Conversely, ITIL and ISO 20000 are very strong in service aspects but lack strategic and innovative approaches [17]. ADIGOV combines both through its three-domain structure, ensuring connectivity between strategy, services, and innovation.

Second, in terms of support for innovation and agility. Frameworks such as PMBOK and CMMI tend to be rigid and unresponsive to technological dynamics and innovative needs. The Adapt domain in ADIGOV explicitly adopts the principles of agility, resilience, and sustainability, which have so far been overlooked. This responds to the challenge of governance agility as emphasized in contemporary literature [35].

Third, regarding the approach to ethics and sustainability. Almost all existing frameworks do not explicitly integrate the values of digital sustainability and technology ethics. ADIGOV incorporates Sustainability & Ethics as a key pillar within the Adapt domain to address contemporary issues such as AI ethics, carbon accountability, and social digital inclusion.

Fourth, consider governance resilience and flexibility. Frameworks such as TOGAF and DevOps are considered inadequate in anticipating VUCA (Volatility, Uncertainty, Complexity, Ambiguity) threats and dynamic regulatory changes. Governance flexibility in ADIGOV allows organizations to adaptively modify decision-making structures in response to disruptions, whether technological or geopolitical in nature. Thus, the ADIGOV model offers a modular, value-oriented, and contextually adaptive IT governance approach that can be applied in both public and private sectors. Mapping the three domains into the strategy–service–innovation cycle makes ADIGOV relevant in supporting sustainable digital transformation

3.3. Practical and Theoretical Implications

Practically, ADIGOV can serve as a reference for organizations in designing or evaluating IT governance systems based on agility and sustainability. The model can be adopted either as a whole or by individual domains, depending on the organization's maturity level and needs. From a theoretical standpoint, ADIGOV extends the scope of IT governance toward "next-generation digital governance", integrating strategic, service, and innovation theories [1]. Furthermore, the model opens new opportunities for developing measurement metrics for governance agility and sustainability maturity, which remain scarce in current literature. The combination of structural elements (domains and processes) with dynamic dimensions (flexibility and innovation) constitutes ADIGOV's main differentiation from conventional frameworks.

4. CONCLUSION

The study successfully formulated a new IT governance model called ADIGOV (Adaptive Digital IT Governance Framework), designed as an adaptive synthesis addressing the weaknesses of eleven leading frameworks, such as COBIT, ITIL, TOGAF, ISO/IEC 38500, and others, which were found inadequate in supporting the holistic integration of strategy, service management, innovation, and digital sustainability. ADIGOV consists of three main domains: Govern, Manage, and Adapt, each accommodating the strategic, operational, and adaptive needs of modern digital organizations. It was developed using a design science research (DSR) approach and validated empirically. From a theoretical perspective, the study expands IT governance discourse by integrating principles of

strategic alignment, agile governance, and digital sustainability into a single modular framework that can be measured through a maturity assessment. From a practical perspective, ADIGOV offers an actionable guide for organizations to design, evaluate, and enhance IT governance systems based on value and risk, while meeting agility demands in the VUCA era. Although the model has been conceptually validated and tested within the context of public sector organizations, its limitation lies in the absence of quantitative validation through longitudinal studies or cross-sector experiments. Therefore, Further research is recommended to test the effectiveness of ADIGOV through multi-organizational empirical studies, develop AI-based maturity assessment tools, and further explore the integration of digital ethics and data governance, particularly quantitative testing with cross-organizational implementation testing. The main contribution of this work is addressing the research question on the need for an IT governance model that integrates core functional domains and is also adaptive, modular, and measurable in supporting sustainable digital transformation.

5. ACKNOWLEDGEMENTS

Thank you to all the leaders of Universitas Pembangunan Nasional Veteran Jakarta, especially to the Faculty of Computer Science, and to all colleagues involved in and supporting the writing and research process.

6. DECLARATIONS

AI USAGE STATEMENT

During the process of compiling this work, the author (authors) used AI assistance to translate (https://www.deepl.com/en/translator) and Litmap (https://www.litmaps.com/) to assist in translating. The author has also reviewed the content for proofreading and used Litmap to assess the progress of similar research and to identify relevant literature. After utilizing these tools/services, the author has reviewed and edited the content as necessary and assumes full responsibility for the content of this publication.

AUTHOR CONTRIBUTION

Bambang Saras Yulistiawan led the conceptualization of the study, including problem formulation and the development of the Adaptive Digital IT Governance Framework, while also coordinating the research team and integrating the various contributions into the final manuscript. **Rifka Widyastuti** was primarily responsible for conducting an in-depth literature review on IT governance and digital transformation, as well as mapping existing governance models to serve as the foundation for the proposed framework. **RR Octanty Mulianingtyas** designed the research methodology, ensured the appropriateness of the analytical approach, and managed the validation of the framework through case study analysis and comparative evaluation. **Galih Prakoso Rizky A** contributed by processing data, conducting empirical analysis, and developing the visual representation of the framework, as well as drafting the results and discussion sections. **Hengki Tamando Sihotang** focused on formulating the practical implications and recommendations for organizational adoption of the framework, while also refining the conclusion and ensuring the overall academic rigor and language consistency of the manuscript.

FUNDING STATEMENT

The research, including all activities throughout the study and the publication process, was entirely self-funded by the authors as a team. No external financial support was received from any public, commercial, or not-for-profit funding agencies.

COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] P. Weill and J. W. Ross, "IT governance: How top performers manage IT decision rights for superior results," pp. 1–105, 2004.

[2] P. Weill and S. L. Woerner, "Thriving in an increasingly digital ecosystem," *MIT sloan management review*, vol. 56, no. 4, p. 27, 2015.

[3] Isaca, "Cobit 5," 2012.

[4] S. de Haes, W. Van Grembergen, and T. Huygh, "Enterprise governance of information technology," pp. 1–566, 2020, https://doi.org/10.1007/978-3-030-25918-1.

[5] F. M. Njiru, "A GIS Audit Framework for Sustainable GIS Applications and Services," pp. 1–302, 2024.

[6] F. Amagoh, "Perspectives on organizational change: systems and complexity theories," *The Innovation Journal: The public sector innovation journal*, vol. 13, no. 3, pp. 1–14, 2008.

[7] I. Graglia, "COBIT vs ITIL: A Comprehensive Comparison for IT Governance," pp. 1–10, 2024.

[8] A. B. Consortium, "Governance for the Agile Organization," *egile bussiness*, vol. 8, no. 3030597, pp. 1–22, 2025.

[9] W. D. Eggers, Paul Bien;, Shannon Lundquist;, Maximilian Lennart Nagel;, and Pankaj Kishnani;, "Government's newfound agility," pp. 1–20, 2024.

[10] N. E. Governance, "GG3030 E NVIRONMENTAL G OVERNANCE I The Dutch National," *Waste Management*, vol. 7, no. 7, pp. 1–8, 2025, https://doi.org/10.1007/978-3-031-36457-0_12.

[11] W. S. de Araujo, "A method for the formulation of E-Governance strategies taking into account international rankings," pp. 1–216, 2022, https://doi.org/10.1007/978-3-031-12673-4_4.

[12] C. R. Rodriguez, J. L. B. Ore, and D. E. Vargas, "Las variables en la metodologia de la investigacion cientifica," vol. 78, pp. 1–231, 2021, https://doi.org/10.17993/IngyTec.2021.78.

[13] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact," *MIS quarterly*, vol. 37, no. 2, pp. 337–355, 2013, https://doi.org/10.25300/MISQ/2013/37.2.01.

[14] S. Mettler, "The submerged state: How invisible government policies undermine American democracy," pp. 1–162, 2011, https://doi.org/10.1080/07393148.2012.754678.

[15] P. Gillespie, "Security Compliance in Large Private Enterprise Information Systems Utilizing DevOps: An Exploratory Study," pp. 1–218, 2024.

[16] L. Al Omari, "IT governance evaluation: adapting and adopting the COBIT framework for public sector organisations," pp. 1–266, 2016.

[17] S. D. Galup, R. Dattero, J. J. Quan, and S. Conger, "An overview of IT service management," *Communications of the ACM*, vol. 52, no. 5, pp. 124–127, 2009, https://doi.org/10.1145/1506409.1506439.

[18] M. Axelos, L. Bamiere, F. Colin, J.-Y. Dourmad, M. Duru, S. Gillot, B. Kurek, M. Jean-Denis, V. Requillart, and J. Mery, "Reflexion prospective interdisciplinaire bioeconomie-Rapport de synthese," pp. 1–300, 2020.

[19] J. Iden and T. R. Eikebrokk, "Using the ITIL process reference model for realizing IT governance: An empirical investigation," *Information Systems Management*, vol. 31, no. 1, pp. 37–58, 2014, https://doi.org/10.1080/10580530.2014.854089.

[20] G. Selig, "Implementing IT Governance-A Practical Guide to Global Best Practices in IT Management," pp. 1–297, 2008.

[21] H. Kerzner and F. P. Saladis, "Project management workbook and PMP/CAPM exam study guide," pp. 1–531, 2017.

[22] M. C. Paulk, "A history of the capability maturity model for software," *ASQ Software Quality Professional*, vol. 12, no. 1, pp. 5–19, 2009.

[23] V. S. S. de Ataide Ramos, "A CMMI-compliant Requirements Management and Development Process," pp. 1–24, 2014.

[24] A. Wiedemann, "IT governance mechanisms for DevOps Teams-How incumbent companies achieve competitive advantages," pp. 1–10, 2018, https://doi.org/10.24251/HICSS.2018.617.

[25] R. Knaster and D. Leffingwell, "SAFe 5.0 distilled: achieving business agility with the scaled agile framework," pp. 1–626, 2020.

[26] M. Tervajoki, "IT Transformation to Support Business Driven Requirements," pp. 1–245, 2017.

[27] Y. Maleh and A. Sahid, "Navigating IT governance for resilient organizations," pp. 1–315, 2024, https://doi.org/10.4018/979-8-3693-3431-7.

[28] J. Becker, B. Niehaves, J. Poeppelbuss, and A. Simons, "Maturity models in IS research," pp. 1–302, 2010.

[29] P. Awasthi and K. T. Tai, "Leadership framework for an agile government," pp. 1–57, 2025, https://doi.org/10.1007/978-3-319-31816-5_4475-1.

[30] J. van de Hoven and Comande.

[31] A. R. Hevner, "A three cycle view of design science research," *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4, 2007.

[32] I. Governance and C. Manajement, "COBIT 2019 Framework: Governance and Management Objectives," pp. 1–302, 2019, https://doi.org/10.29103/jreece.v5i1.19501.

[33] N. Labib, "Mengenal Information Systems Audit and Control Association (ISACA)," 2019, https://doi.org/10.31219/osf.io/m93u8.

[34] O. o. G. Commerce, "Gereciando projetos de sucesso com PRINCE2:[Brazilian Portuguese print version of Managing successful projects with PRINCE2]," pp. 1–365, 2011.

[35] P. Weill and S. L. Woerner, "Is your company ready for a digital future," *MIT Sloan Management Review*, vol. 59, no. 2, pp. 21–25, 2018, https://doi.org/10.7551/mitpress/11859.003.0005.

[This page is intentionally left blank.]