JPPIPA 11(10) (2025)

Jurnal Penelitian Pendidikan IPA

http://jppipa.unram.ac.id/index.php/jppipa/index

Defense Information Systems Architecture for Cyber Threats: A Systematic Review of the Research Literature

Martanto Dwi Saksomo Hadi[1*], Rudy Agus Gemilang Gultom[1], Ansori[1], Bambang Kustiawan[1]

[1] Department of Defense Strategy, Defense University of the Republic of Indonesia, Bogor Regency, Indonesia.

Received: July 30, 2025
Revised: September 20, 2025
Accepted: October 25, 2025
Published: October 31, 2025

Corresponding Author:
Martanto Dwi Saksomo Hadi
martanto.dwis@yahoo.co.id

DOI: 10.29303/jppipa.v11i10.12905

© 2025 The Authors. This open access article is distributed under a (CC-BY License)

Abstract: Cyber threats have become a serious challenge to national defense. Although Indonesia has a high cybersecurity index, a series of significant incidents against government institutions indicate urgent vulnerabilities that need to be addressed through a more resilient defense architecture. This study conducted a systematic literature review (SLR) to identify the results and practices of implementing the TOGAF, DoDAF, and COBIT (TDC) frameworks in the cyber defense domain. The results indicate that the literature is dominated by qualitative studies (53%) and COBIT framework implementations (73%), especially in government agencies (67%). The analysis yielded four main themes: improved governance and compliance, optimized risk management, strengthened security posture, and architectural and operational efficiency. The literature's focus on the first two themes signals a strategic shift from technical solutions to a governance- and risk-based approach. The study concludes that an effective approach to modern cyber defense is through integrating the specific strengths of each framework: COBIT for governance, DoDAF for operations, and TOGAF for architecture.

Keywords: Cyber risk; Cyber security; Cyber threats; Security architecture; Security resilience

Introduction

Advances in information and communication technology have a positive impact as well as a serious threat in the context of national defense (Kshetri, 2005; Septipalan et al., 2024; Yasmin & Yulianto, 2024). Battlefield transformation in the cyber realm has become the fifth domain after land, sea, air and space (Ariyadi & Rizky Pohan, 2023; Juliana et al., 2024; Siroli, 2018). Asymmetric cyber threats demand that the country's defense strategy adapt through the development of resilient, adaptive and layered information systems (Farhaoui et al., 2024; Marvin Immanuel et al., 2024).

The technological paradox gives rise to threats such as supply chain attacks that subvert traditional concepts of territorial integrity and security (conventional warfare), thus requiring a comprehensive understanding of vulnerabilities in interconnected infrastructures (Bardin, 2024). As one example that the fifth domain of the universe is also a serious threat to the defense of a country is the war between Russia and Ukraine which has occurred on a full-scale since 2022 (Pandey & Kumar, 2023). The war between Russia and Ukraine is essentially a hybrid war that integrally combines physical and cyber dimensions targeting a wide range of critical infrastructure, ranging from physical cyber systems to general computing networks, the objectives of these cyber operations are very diverse including attempts at destruction or disruption of services, data theft, as well as the dissemination of unexpected information either intentionally or unintentionally (Noor et al., 2023; Pandey & Kumar, 2023; Siregar et al., 2024).

This condition is relevant globally, including in Indonesia, Indonesia's cyber defense received a high score of 95-100 which was classified as "Role-modelling"

How to Cite:
Hadi, M. D. S., Gultom, R. A. G., Ansori, & Kustiawan, B. (2025). Defense Information Systems Architecture for Cyber Threats: A Systematic Review of the Research Literature. *Jurnal Penelitian Pendidikan IPA*, *11*(10), 10–22. https://doi.org/10.29303/jppipa.v11i10.12905

in cyber defense according to the Global Cybersecurity Index including 4 other Asian countries such as Vietnam, Malaysia, Singapore, and Thailand (International Telecommunication Union, 2024; Tristantie & Dwi Nitami, 2024). Even though Indonesia is one of the countries that has a good level of cyber security in Southeast Asia, cyber attacks are still dangerous in Indonesia because several cases prove that the cyberattacks have succeeded in attacking the defense system in official government institutions such as breaking into access to the YouTube account of the Indonesian House of Representatives (DPRI) in 2023 (Aji & Artikel, 2023), leak of State Civil Apparatus (ASN) data at the National Data Center (PDN) in 2024 (Al Baihaqy et al., 2024), the 2024 Provisional National Data Center (PDNS) data leak that caused a number of government services, including immigration, to experience major disruptions (Ghalib et al., 2024), and the leak of NPWP data in 2024 at the institution of the Directorate General of Taxes (DGT) under the Ministry of Finance (Kusnadi, 2021).

This vulnerability is not only a problem experienced by developing countries. Even countries with leading technological and military power such as the United States with a Power Index (PwrIndx) of 0.0744, which is the country with the highest technological and military power in the world, followed by Russia and China, which have the same PwrIndx value, namely 0.0788, where the reference number of 0.0000 is a perfect PwrIndx value that is impossible for any country to achieve (Global Fire Index, 2025). Nevertheless, cyber attacks can still occur in the United States. Several states such as California, Texas, Florida, New York, and New Jersey suffered losses of $3,089,000,000 due to cyber attacks (Sentinel One, 2025). This shows that superiority in the conventional realm does not necessarily guarantee security in the cyber realm. Therefore, preparing a robust defense system architecture is a crucial preventative measure to maintain national stability from modern threats. This architecture must be designed to consistently address cyber threats, which continue to evolve along with advances in information technology. Therefore, it is necessary to prepare the best defense architecture as a preventive measure against cyber attacks that can disrupt the stability of the country (Lehto, 2022).

This research is highly relevant considering the current situation in Indonesia. Although the Global Cybersecurity Index classifies Indonesia's cyber defenses as high in the “Role-modeling” category, a series of significant cyber incidents have revealed pressing vulnerabilities. Various vital government institutions have been hacked, such as the hacking of the House of Representatives (DPR) YouTube account in 2023, the leak of Civil Servant (ASN) data at the National Data Center (PDN) in 2024, the disruption of immigration services due to an attack on the Temporary National Data Center (PDNS) in 2024, and the leak of Taxpayer Identification Number (NPWP) data at the Directorate General of Taxes (DGT) in 2024. This series of attacks demonstrates the gap between international recognition and cyber defense capabilities in the field. Failure to protect strategic data assets and public services is not only financially detrimental but also threatens sovereignty and public trust (Hadiati & Pramuda, 2024; Wibisono, 2023). Therefore, research to build a more integrated and robust defense architecture model is an urgent need.

National Defense

Indonesian state defense in article 1 paragraph 2 of Law (UU) Number 3 of 2002 concerning State Defense is universal which involves all citizens and all regions which must be prepared early and organized in total by the government to uphold state sovereignty, territorial integrity and the safety of the entire nation from all threats (Government of the Republic of Indonesia, 2002). Defense system architecture is defined as a framework concept that will seek the best defense of the country (Garrett et al., 2011). In the defense architecture, there is also a framework to address cyberattacks as the fifth domain that has been recognized (Safitra et al., 2023). The defense information system architecture must always be improved to be adequate to deal with modern cyber threats that are increasingly developing along with the increasing capabilities of today's information technology (Steingartner et al., 2021).

TOGAF, DoDAF and COBIT (TDC) Defense System Architecture

State defense as a vital object of state sovereignty, the researchers remind the importance of an effective defense architecture for state defense (Costa et al., 2024; Jardim et al., 2022; Mustopo et al., 2024). The researchers identified several defense architectures that have been tested commonly used as Information Technology (IT) governance and globally recognized as TOGAF (de Oliveira etf al., 2021), DoDAF (Wang et al., 2024), and COBIT which is summarized as (TDC) in this study in order to provide a management framework that can be applied to the management of defense systems (Bhatia et al., 2023; Gaudêncio et al., 2024; Juma et al., 2023). The research will seek to combine the three popular frameworks to build a conceptual architecture foundation on better defense aspects that can address the latest attacks such as cyberattacks.

The Open Group Architecture Framework (TOGAF) is a corporate architecture framework with a main focus on designing, planning, implementing, and managing information technology architectures that can be adapted by the private industry and government in every phase that integrates the Architecture Development Method (ADM) (Hidayat et al., 2024). TOGAF ADM begins with the establishment of basic security principles in the early stages which are then aligned with the business vision in phase A. The core of the architecture design (Phases B, C, and D) involves the deep integration of security at the business, data, application, and technology levels through concrete activities such as threat modeling and data classification. The final stages, from implementation planning to governance and change management (Phases E to H), ensure that the security architecture that has been designed can be realized consistently and is able to adapt to various threat developments (Hidayat et al., 2024).

The Department of Defense Architecture Framework (DoDAF) is a military framework for planning complex operations by ensuring all systems, such as weaponry and communications, can work together effectively. DoDAF is often used to build short-term architectures that are specific to each mission, such as hostage release or cyberattacks (Wang et al., 2024). The implementation process begins with defining mission objectives, continues with mapping out the tasks and who is involved and ends with selecting the right technology (Wang et al., 2024). The result is a complete picture of operations to analyze to find deficiencies, ensure all systems are connected, and reduce risk before the mission is executed (Wang et al., 2024).

Control Objectives for Information and Related Technologies (COBIT) is an IT governance and management framework that focuses on the control, risk management, and value creation of technology. The framework serves as a comprehensive guide for auditors, managers, and executives to ensure IT strategies align with business objectives, risks are effectively managed, and technology investments are proven to deliver optimal outcomes for organizations.

The application of COBIT in a mission is carried out systematically through three main phases that cover the entire technology life cycle. First, at the planning and preparation stages of the Align, Plan, and Organize (APO) and Build, Acquire, and Implement (BAI) domains. The APO domain manage strategy will ensure that the technology strategy (e.g., the use of drones, communication networks, data analysis systems) actually supports the mission's main objectives. APO manage risk will identify and evaluate IT-related risks such as possible risks of communication being intercepted, navigation systems failing. APO budget and resource management will ensure that the allocation of funds and IT personnel for the mission is efficient and as needed. If the APO domain is the framework for the entire operation then the BAI domain will build and implement the solution in a mission to be built, tested, and implemented securely and to specification. For example, ensuring that the command and control systems have passed safety testing before being used in the field.

Second, during the execution of the Deliver, Service, and Support (DSS) mission the focus shifts to operations, where COBIT guarantees all systems are running reliably, any technical incidents are handled quickly, and cybersecurity is maintained actively and in real-time. For example, if a cyberattack occurs at the command network center, the DSS domain will take steps where the cybersecurity team immediately isolates the threat, blocks access, and restores the system without disrupting the surveillance operation.

Finally, in the evaluation stage after the mission is completed Monitor, Evaluate, and Assess (MEA), COBIT is used to measure technology performance, verify compliance with all rules, and identify valuable lessons for future improvements. The monitoring and evaluation process will be a thorough assessment of the technology after it is used in the mission. This process includes an analysis of the performance and value provided by the technology, such as whether the system is running fast and reliable. In addition, an evaluation was also carried out on the effectiveness of the security and operational controls that have been implemented to find loopholes for improvement. And this process ensures that the use of technology during missions has complied with all applicable internal policies and legal regulations.

TDC Research Review in the field of Defense Systems

Recent reviews of research related to TDC contain limitations and limitations. In line with the development of wars with a cyber dimension, some of them (Douzet & Gery, 2021; Liebetrau, 2022; Willett, 2023) has seen a different perspective from the shift of conventional physical warfare to the serious threat of technology in the form of cyber warfare. In addition, this review focuses on the effects of cyberattacks on the geopolitical aspect where the country must see this cyberattack as a domain of confrontation between countries for national security and the systematic aspect where the effects of cyber attacks such as malware on the system can threaten the stability of the country, European countries such as France, the Netherlands, Norway do not yet have a coherent strategic framework for this cyber threat because it focuses on conventional warfare.

Other related reviews have examined TDCs where COBIT and TOGAF can be used simultaneously (Seyboth & Beckmann, 2024), but requires further research on the joint operational implementation of multiple frameworks and studies of industry-specific frameworks that may be more effective. Dissertation from Carolina et al. (2023) stating that traditional frameworks are inadequate to model the interactions, data flows, and digital opportunities that arise from cross-company collaboration in a single sectoral supply chain, so a new framework tailored to needs is needed.

To address these challenges, various architectural frameworks such as TOGAF, DoDAF, and COBIT have been widely used for Information Technology (IT) governance and defense. However, previous research tends to have limitations. Some studies examine these frameworks separately or simply combine the two frameworks, leaving open the need for further research on more comprehensive, joint operational implementations. Other studies even conclude that traditional frameworks are often inadequate for modeling the complex interactions and data flows involved in modern cyber threats, necessitating a new framework tailored to specific needs. Our study of the TDC framework highlights the need for the integration of joint frameworks to meet specific needs and meet the challenges of cyber warfare.

Motivated by gaps highlighted by other studies and based on ongoing questions from personnel, institutions, and policymakers, we conducted a systematic review of the TOGAF, DoDAF, and COBIT (TDC) defense system architecture literature with the goal of examining empirical outcomes related to effectiveness and efficiency. Specifically, we sought to identify key outcomes and practices of interest in TDC studies and contextualize our findings within broader defense system trends. The novelty of this research lies in its approach of conducting a systematic literature review (SLR) that specifically examines the combined implementation outcomes and practices of three key frameworks TDC in the cyber defense domain. This research fills a gap in the literature by not focusing solely on one or two frameworks, but rather synthesizing the strengths of all three to build a foundation for a more integrated conceptual architecture model. Thus, this research aims to identify best practices and empirical outcomes from the application of these three frameworks as a foundation for designing a more holistic, adaptive, and resilient cyber defense architecture against modern threats. The primary research question guiding our review is, in TDC (focused on defense against cyber attacks), what positive and negative practices are mentioned in the published literature? To answer this question, we first identify TDC practices in the defense domain that are expected to be reported in published TDC research, leading to the identification of two supporting research questions: (a) what are the outcomes of TDC framework implementations in the cyber defense domain that have been reported in these studies? and (b) what implementations have been reported in published TOGAF, DoDAF, and COBIT research in cyberspace?

Method

We adopt a broad conceptualization of TDC that includes effectiveness and efficiency with the aim of creating a new framework that is applicable to the challenges of cyberattacks. The perspective that different types of frameworks provide a diverse range of cyber defense experiences globally will guide the design, implementation, and analysis of our review (Katsantonis et al., 2023; Perwej et al., 2021).

Design and Process of Systematic Review Search

Our systematic literature review research follows the generally recognized guidelines of PRISMA 2020 which describe the reporting criteria, the researcher reserves the right to determine the number of words, the number of sections, and the maximum number of tables and images that can be included in the main article (Dehesh, 2024; Nezameslami et al., 2024; Parums, 2021). We use 6 academic databases, Scopus, Taylor & Francis Online, JSTOR, IEEE Xplore, ACM Digital Library. We used three sets of search terms in six academic databases. The term set will narrow the scope to studies focusing on TOGAF, DoDAF and COBIT defense systems (see Table 1). We select search terms through a review of the titles, abstracts, and keywords of articles that have been identified as relevant in consultation with expert advisors in the field of defense and cybersecurity. The search terms in each set are separated by the “OR” operator and the two sets of search terms are combined using the “AND” operator We are looking for studies published between 2022 to 2025, a period that aligns with the review published and corroborated by our expert advisory panel (Table 1 and Figure 1 detail the process, the latter including a PRISMA Flowchart for the search and screening process). Through an automated search process, we remove duplicate data in each database once it has been compiled. The results of the search strategy (database search) resulted in a total of 372 data.

Data Screening and Feasibility

Sifting through 372 data, we read each abstract and used a decision tree to identify relevant studies based on inclusion criteria, namely the data is a scientific article, the publication year range is between 2022 and 2025, focusing on cyber defense in 3 frameworks TOGAF, DoDAF, and COBIT.

The TOGAF, DoDAF, and COBIT framework reports are intended to review broadly to achieve a new conceptuality in the architecture of cyber defense systems. The initial screening process excludes publications that are oriented not to scientific articles such as theses, theses, and dissertations. Furthermore, through an abstract review, we eliminated 317 data that did not meet the criteria, for example because they were outside the specified publication year range or focused on a different topic. Of the remaining 317 articles, we conducted a full-text review. After this in-depth evaluation, 40 articles were again excluded because they were found not to meet the inclusion criteria.

Table 1. The Search Term Used in Database Searches

TOGAF	Operator	DoDAF
"TOGAF" OR "DoDAF" OR "COBIT"	AND	"cyber" OR "effectiveness" OR "efficiency"

Note: The asterisk "" is a word cutting symbol, which directs search engines to find a specific word shape.

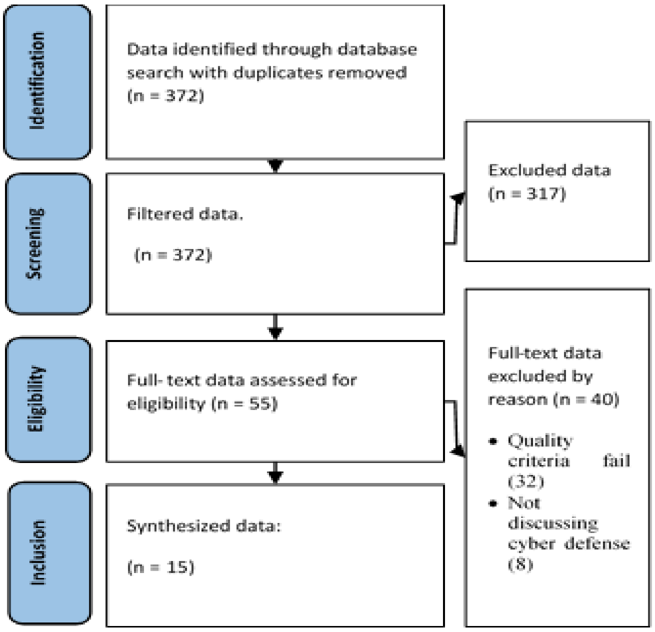
Identification
Data identified through database search with duplicates removed (n = 372)
Screening
Filtered data. (n = 372)
Excluded data (n = 317)
Eligibility
Full- text data assessed for eligibility (n = 55)
Full-text data excluded by reason (n = 40)
• Quality criteria fail (32)
• Not discussing cyber defense (8)
Inclusion
Synthesized data: (n = 15)

Figure 1. Prisma flowchart, based on the provisions of prisma (Parums, 2021)

Quality Assessment

Quality assessment is carried out with several factors. We employ experts to provide external feedback throughout the process, our review team is made up of experts in research methodology and with previous experience in conducting systematic reviews. The quality criteria we have previously established include ensuring that the study provides relevant information, basic information about the research methods and data, and sufficiently detailed findings. We chose this criterion because our review was designed to be configurative, not aggregative, with a focus on identifying the efficiency and effectiveness of the TDC framework. In addition, we chose to only include peer-reviewed articles in our final sample, as the process proves that a quality assessment has been conducted. In addition, we specifically look for articles that adequately describe the methods and sizes of research as well as data collection tools/instruments, and present clear data to support claims. The research team met to discuss opinions and quality evaluations for each study and ensure consistent application of quality criteria. During the quality review, team members agreed on four studies that did not meet the quality criteria. The final sample includes 15 scientific articles.

Data Analysis

The analysis was carried out thematically, as described by Braun et al. (2023), involves data recognition by reading and identifying findings, initial code, grouping themes, defining themes, and writing findings with found evidence. The articles in our final sample represent a diverse range of research designs that produce qualitative and quantitative data, we use a systematic synthesis review approach on qualitative research followed by thematic analysis methods (Vors & Bourcier, 2022; Younas et al., 2021). The method of thematic analysis, as well as explicitly stating the themes that emerge from the selected literature and detailing how the qualitative synthesis is structured (e.g., the thematic encoding of the advantages of the TDC framework). Sources are categorized based on these themes, ensuring a structured synthesis of findings. This approach allows for a deeper contextual understanding of complex issues such as TDC adoption across a wide range of industries with a focus on cyber defense.

In order for data extraction to be easily understood, a code book that mentions and describes the main coding categories of interest and provides sample code we create in a table (Hilmi et al., 2023). We tested all the code and resolved any discrepancies through group discussions, and reached 100% agreement on the coding decision before proceeding to fully code a comprehensive research suite. To do so, we use a manual iterative process to modify the codebook based on emerging trends. We add, revise, and rearrange code until we reach a code usage agreement point.

Table 2 coding, we aggregate data that allows us to identify trends in the data (Lee et al., 2024). We code data categories based on the framework, using combinations to manage processes across data sets. Coding is carried out on all articles with the categories of country, year, implementation, type of framework, publication channel, type of research, research results, overall findings. The data provide a general description of the results of the framework included in the final sample. We then construct the synthesis in an inductive manner as we prioritize predefined practices related to the efficiency and effectiveness of the TDC framework.

Table 2. Coding Categories for Data Extraction and Analysis

Categories Coding	Explanation	Code Examples
Country	Name of the country where the research was conducted	Indonesia, United States
Year	Year the article was published	2021, 2022, 2023
Implementation	Description of where the research was conducted	Defense Industry, Command Center
Types of Frameworks	Description of the framework used	TOGAF, DoDAF, COBIT
Publication Channels	Description of the journal in which the study was published	Journal of Information Systems
Types of Research	Types of research conducted based on methods and data	Quantitative, qualitative, mixed methods
Research Results	Types of results reported by the author	Can or may not be implemented on cyber threats
Overall Findings	General level of reported results	Positive, negative, null

Result and Discussion

Results

The 15 research articles in the final review were published across three journal themes: computing, engineering and technology, and defense, all focusing on cybersecurity defense frameworks, or the development of defense frameworks and systems. The results show that none of the articles in our sample were published before 2022, and only two (13%) were published in the first half of the period before 2024. Thirteen articles (87%) of the final sample were published between 2024 and 2025 (see Figure 2).

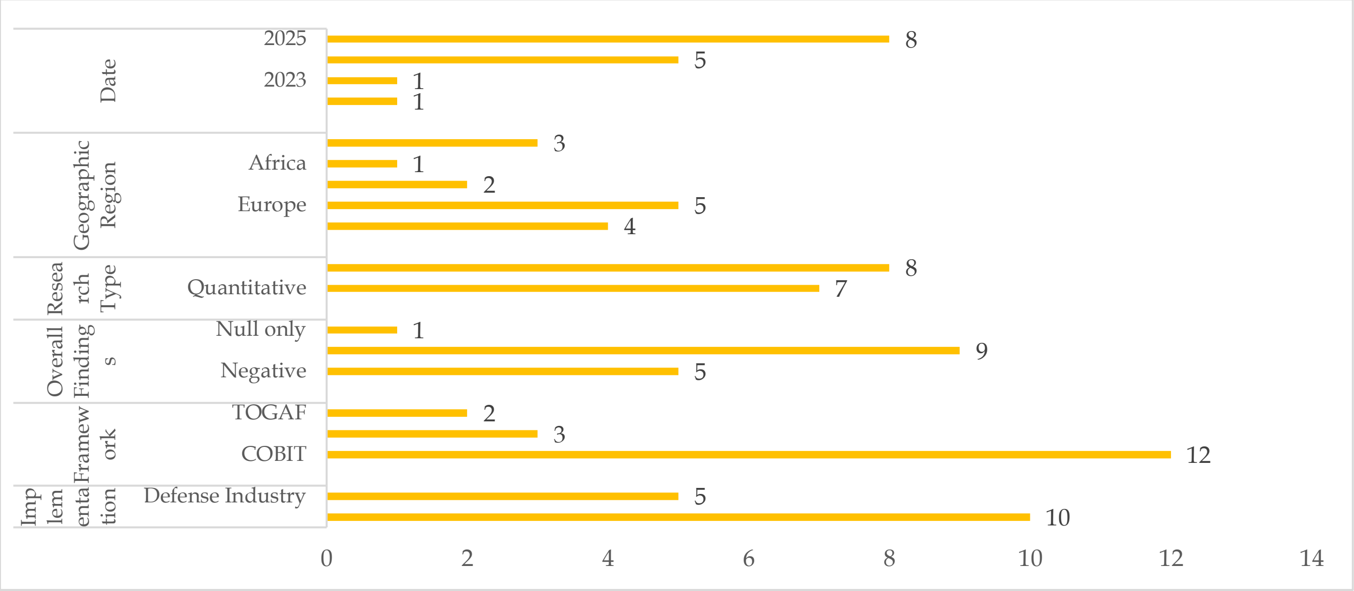

Figure 2. Research characteristics of the reviewed article

Figure 2 shows the general characteristics of the reviewed literature. Geographically, research is dominated by studies from Europe (33%) and Asia (27%). Methodologically, there is a strong skew toward qualitative research, with 8 articles (53%) focusing primarily on qualitative data, and 7 (47%) on quantitative data. Regarding reported results, the majority of studies (9 articles (60%) demonstrated positive findings from the application of the framework, with only 5 (33%) reporting negative results and 1 (7%) reporting no significant impact.

In terms of frameworks applied, COBIT is significantly the most discussed, appearing in 11 articles (73%) while the remaining 4 articles (27%) discuss the TOGAF and DoDAF frameworks, the COBIT and TOGAF frameworks simultaneously are present in 1 article, there are also 2 articles that discuss DoDAF specifically and 1 article discusses DoDAF and TOGAF simultaneously, TOGAF is not specifically discussed in one article but a combination of several frameworks such as TOGAF and COBIT in 1 article and TOGAF and DoDAF in 1 article. In terms of framework implementation, the majority of its application is in the government agency environment (67%), compared to the defense industry or military sector (33%).

Discussion

In order to answer the formulation of the research problem, we formulated four thematic classifications for the results found in the literature. These categories, which are inductively excavated from relevant studies, include: (1) Improved Governance & Regulatory

Compliance. (2) Optimization of Cyber Risk Management. (3) Strengthening Posture and Security Resilience, and (4) Architectural and Operational Efficiency.

Table 3 shows that the majority of findings we analysed centered on the first two categories, highlighted in 15 studies (approximately 53%) or 8 findings articles in this domain, for example by "achieving better regulatory compliance" and "having a more structured threat identification process". Meanwhile, several other studies reported impacts on Strengthening Security Posture and Resilience (33%), such as "faster incident response times" and "increased visibility into critical assets". Findings related to Architectural and Operational Efficiency appeared with less frequency (13%), with examples being "standardization of workflows" and "elimination of redundancies in systems".

Table 3. Summary of Main Themes and Their Frequency from Reviewed Articles

Categories Coding	Number of articles (% of the entire sample)	Subcategories
Improved Governance & Regulatory Compliance	53	Achieving better regulatory compliance
Cyber Risk Management Optimization		A more structured threat identification process
Posture Strengthening and Security Resilience	34	Accelerated incident response time, Increased visibility on critical assets
Architectural and Operational Efficiency	13	Standardization of workflows

a. Based on the decreasing frequency (n = 15).

Improved Governance & Regulatory Compliance

A significant portion of the literature reviewed shows that architecture and cybersecurity frameworks play an important role in establishing and maturing information technology (IT) and security governance functions. Frameworks such as COBIT are often the first choice to ensure structure, accountability, and alignment with organizational goals (Arimurti et al., 2024; Bernika et al., 2021; Nasiri, 2023; Nugraha & Hendrik, 2024). Research such as Russo et al. (2024) highlights how COBIT provides a comprehensive IT governance framework to align IT with business strategy, optimize resources, and manage risk.

Furthermore, this framework is a measuring tool and guide to achieve compliance with applicable standards and regulations. Study by McIntosh et al. (2024) using CMMI and COBIT to evaluate the maturity of security governance, ultimately helping organizations achieve compliance with security standards. This is reinforced by research Proudfoot et al. (2025) which explicitly offers a governance model to help organizations comply with various existing regulations. The function of measuring the level of maturity as part of governance is also emphasized by Fadya & Utama (2025) which uses a combination of NIST CSF and COBIT 2019 to measure and improve an organization's security maturity.

However, the roles of TOGAF and DoDAF are also crucial in achieving effective governance (Kartika & Yolanda, 2024; Putra & Anggreani, 2022). TOGAF acts as a bridge that translates high-level governance policies (defined by COBIT) into concrete architectural blueprints. Through the Architecture Development Method (ADM), TOGAF ensures that compliance and governance requirements are integrated early in the design of business, data, application, and technology architectures. Meanwhile, DoDAF ensures that these governance principles are effectively implemented at the operational level. In the context of specific military missions, DoDAF provides Operational Views (OVs) and System Views (SVs) that visualize how an operation complies with established rules, ensuring compliance in the execution of missions in the field.

Cyber Risk Management Optimization

Risk management optimization is the second central theme that emerges from the analysis. The framework provides a systematic approach and methodology for identifying, assessing, and managing cyber risks, thereby moving organizations from a reactive approach to a more proactive one. Research by Ali et al. (2024) specifically recommends the OCTAVE Allegro methodology for conducting risk assessments to effectively identify and manage cyber threats within the COBIT framework.

A focus on risk reduction as a tangible end result is also reported (Ghozie Afiansyah et al., 2023; Lestari et al., 2024; Ramadhanty, 2024). Study by Fadya et al. (2024) found that the implementation of the NIST CSF framework can significantly reduce cyber risk, one of which is by encouraging better collaboration between stakeholders. This theme is not only limited to assessment, but also to the development of a sustainable risk management program (Balafif, 2023; Julianto et al., 2024; Ramadhanty, 2024). Research McIntosh et al. (2024) explore best practices in this domain on the COBIT framework to help organizations build effective risk management programs over the long term.

TOGAF role in this theme is proactive, managing risk at the architectural level (Mulyana et al., 2024;

Vernandy & Herdi, 2023). During the design phase (Phases B, C, and D), TOGAF integrates threat modeling and risk analysis to build security directly into the architecture, rather than as an add-on. This enables the identification and mitigation of architectural vulnerabilities before they are exploited (Elysia et al., 2024; Putra et al., 2024). DoDAF, on the other hand, manages risk at the operational and mission levels (Stephanie et al., 2024). The framework is used to model interdependencies between systems within an operation, enabling the analysis of mission-specific risks, such as communications system failure or data interception, and ensuring all risks are mitigated before the mission is executed.

Posture Strengthening and Security Resilience

In addition to the managerial aspects, many studies report the positive impact of the implementation of the framework on operational and technical capabilities (Safarudin, 2021). It encompasses the entire security lifecycle, from identification to recovery, which collectively strengthens security posture and resilience (Khusumawati, 2024). Some studies have focused on improving detection and response capabilities. Li et al. (2024), presents a structured guide to building an effective cyber defense system, including security monitoring, threat detection, and incident response through the DoDAF framework. Similarly, Lubis et al. (2025) Propose a multi-layered defense model to detect and respond to threats more effectively.

Increased defense capabilities in general are also in the spotlight (Isdiyanto, 2024), as shown by Aghamohammadpour et al. (2023) which develops a technically-oriented approach to strengthen cyber defenses and helps analysts deal with incidents with the DoDAF framework. Ultimately, the goal of posture strengthening is to achieve endurance (Resilience). This theme is explicitly discussed by Busch et al. (2025) which offers a framework for measuring and improving cyber resilience, which is defined as an organization's ability to survive and recover from cyberattacks.

TOGAF contributes to security resilience from a strategic and long-term perspective. By designing a structured and modular enterprise architecture, TOGAF helps create inherently more resilient systems, reduces single points of failure, and simplifies security management across the organization. Meanwhile, COBIT ensures that processes for maintaining a robust security posture are actually implemented and continuously monitored (Fatin et al., 2024). Through the Deliver, Service, and Support (DSS) and Monitor, Evaluate, and Assess (MEA) domains, COBIT provides controls to ensure incident response plans are regularly tested and security performance is continuously measured (Hambali, 2021), as implied by a study by Busch et al. (2024) on cyber resilience measurement.

Architectural and Operational Efficiency

Although it comes with lower frequencies, this theme highlights the important role of frameworks in creating an integrated and efficient security architecture (Dwi Shandika, 2024). Instead of having separate security controls, frameworks like TOGAF help integrate security into business processes and system development lifecycles (Firnaldo et al., 2023). Research by Konnon et al. (2023) demonstrates how TOGAF can be used to provide comprehensive guidance that integrates cybersecurity into the entire system development lifecycle.

This approach results in a more cohesive and holistic architecture (Busch & Zalewski, 2024). It offers a comprehensive cybersecurity architecture model that integrates various security technologies and processes to support more reliable systems. This is in line with a literature review by Barkat Ullah et al. (2024), which also results in a comprehensive security architecture model based on in-depth analysis. Overall, the theme emphasizes how frameworks can prevent security silos and generate operational efficiencies through structured architectural design (Hutagalung et al., 2024).

The DoDAF focuses on achieving operational efficiencies. By providing a clear and standardized view of complex operations, the DoDAF ensures interoperability and synergy between various systems, personnel, and data flows, resulting in more effective and efficient mission execution. COBIT's role in this theme is as a governance framework that ensures that architecturally (by TOGAF) and operationally (by DoDAF) designed efficiencies can be measured and accounted for (A'yuni et al., 2023). COBIT provides metrics to assess whether technology investments are delivering optimal value and whether resources are allocated efficiently, which aligns with the primary objectives of IT governance (Yolanda et al., 2023).

Conclusion

This systematic literature review examines the implementation of the TOGAF, DoDAF, and COBIT (TDC) frameworks in the cyberdefense domain. The analysis of 15 articles indicates that the implementation of these frameworks tends to yield positive outcomes, with a significant implementation focus on government agencies and the defense industry. Thematic analysis classifies implementation outcomes into four main categories. The reviewed literature predominantly highlights the role of COBIT in establishing robust governance and risk management. Other emerging themes, such as strengthening cybersecurity posture and resilience and architectural and operational efficiency, indicate the important role that operationally focused frameworks like DoDAF and architectures like TOGAF can play. The literature's predominant focus on governance and risk signals a strategic shift from purely technical cyber solutions to more structured, management-based approaches. Based on these findings, it is recommended that practitioners consider an integrated approach that combines the strengths of each framework, such as leveraging COBIT for governance foundations, TOGAF for enterprise architecture planning, and DoDAF for mission-critical operational needs. Recommendations for future researchers include addressing the literature gap by examining the effectiveness of combined implementations of multiple frameworks, expanding the research context to the private defense industry, and conducting more quantitative studies to complement the current predominance of qualitative data. It should be acknowledged that the generalizability of these findings has limitations. This review was limited to literature from six academic databases within a narrow timeframe (2022–2025) and was based on a relatively small sample (15 articles). Furthermore, this review did not include gray literature such as theses or dissertations, which could have provided additional insights. These limitations define the scope of this review and open up opportunities for broader systematic research in the future.

Acknowledgments
The author would like to thank all parties who assisted in this research.

Author Contributions
Conceptualization, M.D.; methodology, M.D., R.A., A.A., B.K.; software, M.D.; validation, R.A., A.A. and B.K.; formal analysis, M.D.; resources, M.D.; data curation, M.D.; writing—original draft preparation, M.D.; writing—review and editing, M.D., R.A., A.A., B.K.; visualization, M.D.; supervision, R.A., A.A., B.K.; funding acquisition, M.D. All authors have read and approved the published version of the manuscript.

Funding
This research did not receive external funding from any party; all costs were borne by each author personally.

Conflicts of Interest
We the authors declare that there is no conflict of interest with any party.

References

A'yuni, A. Q., Muhammad, A. H., & Nasiri, A. (2023). Literature Review Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019. *Jurnal Informa : Jurnal Penelitian Dan Pengabdian Masyarakat*, *9*(1), 47–52. https://doi.org/10.46808/INFORMA.V9I1.247

Aghamohammadpour, A., Mahdipour, E., & Attarzadeh, I. (2023). Architecting threat hunting system based on the DODAF framework. *Journal of Supercomputing*, *79*(4), 4215–4242. https://doi.org/10.1007/s11227-022-04808-6

Aji, M. P., & Artikel, R. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/JP.V13I2.3299

Al Baihaqy, A. H., Yuwana, M. A. S. A., Surya, A. P. A., & Fauzi, M. A. N. (2024). Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 dalam Perspektif HAM. *Wicarana*, *4*(1), 31–37. https://doi.org/10.57123/WICARANA.V3I1.167

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*, *00*(00), 1–28. https://doi.org/10.1080/08874417.2024.2329985

Arimurti, N. A., Nurtrisha, W. A., & Falahah, F. (2024). Penilaian Kapabilitas Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 2019 dengan Fokus Domain APO pada RSPAU Dr. Suhardi Hardjolukito. *Jurnal Teknologi Dan Manajemen Informatika*, *10*(1), 13–23. https://doi.org/10.26905/JTMI.V10I1.10939

Ariyadi, T., & Rizky Pohan, M. (2023). Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators. *Jurnal Penelitian Pendidikan IPA*, *9*(12), 10768–10775. https://doi.org/10.29303/JPPIPA.V9I12.5551

Balafif, S. (2023). Penyesuaian Model Ketahanan Siber UMKM di Indonesia Dengan NIST Cybersecurity Framework. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(3), 291–301. https://doi.org/10.30591/JPIT.V8I3.5662

Bardin, J. S. (2024). Cyber Warfare. In *Computer and Information Security Handbook* (4th ed., Vol. 2, pp. 1345–1380). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13223-0.00087-4

Barkat Ullah, A., Ma, W., Ahmed, M., Rashid, B., Saeed, M. A., Arshad, O., & Raghav, U. (2024). A comprehensive review of cyber security and current practices in global mining critical infrastructure. *Journal of Cyber Security Technology*, *00*(00), 1–27.

https://doi.org/10.1080/23742917.2025.2475563

Bernika, H., & I Kadek, D. N. (2021). Perancangan Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 (Studi Kasus: LPP RRI Madiun). *Journal of Emerging Information Systems and Business Intelligence*, *2*(3), 63–70. https://doi.org/10.26740/JEISBI.V2I3.41630

Bhatia, K., Pandey, S. K., & Singh, V. K. (2023). Enterprise Architecture Frameworks for Security Establishment. *2023 International Conference on Artificial Intelligence and Smart Communication, AISC 2023*, 11–17. https://doi.org/10.1109/AISC56616.2023.10085439

Braun, V., & Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. *International Journal of Transgender Health*, *24*(1), 1–6. https://doi.org/10.1080/26895269.2022.2129597

Busch, N. R., & Zalewski, A. (2024). A Systematic Literature Review of Enterprise Architecture Evaluation Methods. *ACM Computing Surveys*, *57*(5). https://doi.org/10.1145/3706582

Carolina, A., & Bandeira, R. (2023). *Towards A Sectoral Enterprise Architecture Framework Seaf* (Issue July). University of Coimbra.

Costa, J. C., Roxo, T., Proença, H., & Morais Inácio, P. R. (2024). How Deep Learning Sees the World: A Survey on Adversarial Attacks & Defenses. *IEEE Access*, *12*, 61113–61136. https://doi.org/10.1109/ACCESS.2024.3395118

de Oliveira, K. V., Fernandes, E. C., & Borsato, M. (2021). A TOGAF-based Framework for the Development of Sustainable Product-Service Systems. *Procedia Manufacturing*, *55*(C), 274–281. https://doi.org/10.1016/J.PROMFG.2021.10.039

Dehesh, P. (2024). Scientific writing in a systematic review and Meta-Analyses. In *Systematic Review and Meta-Analysis: Stepwise Approach for Medical and Biomedical Researchers* (pp. 195–208). Academic Press. https://doi.org/10.1016/B978-0-443-13428-9.00017-3

Douzet, F., & Gery, A. (2021). Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace. *Journal of Cyber Policy*, *6*(1), 96–113. https://doi.org/10.1080/23738871.2021.1937253

Dwi Shandika, M. (2024). Peran Arsitektur Data dalam Meningkatkan Efektivitas Tata Kelola Data di Era Transformasi Digital. *Jurnal Ilmiah Research Student*, *2*(2), 191–195. https://doi.org/10.61722/JIRS.V2I2.5441

Elysia, C., Dethan, T., Clairine, J., Lolong, N., Wandi, S. A., & Kusmana, T. P. (2024). Perencanaan Metode TOGAF dalam Digitalisasi Pasar Swayalan melalui Integrasi Enterprise Architecture. *Jurnal Komputer, Informasi Dan Teknologi*, *5*(1), 15–15. https://doi.org/10.53697/JKOMITEK.V5I1.2573

Fadya, M., & Utama, D. N. (2024). Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019. *TEM Journal*, *14*(1), 182–191. https://doi.org/10.18421/TEM141-17

Farhaoui, Y., Allaoui, A. El, Amounas, F., Mohammed, F., Ziani, S., Taherdoost, H., Triantafyllou, S. A., & Bhushan, B. (2024). A Multi-layered Protection System for Enhancing Data Security in Cloud Computing Environments. *Lecture Notes in Networks and Systems*, *1353 LNNS*, 559–568. https://doi.org/10.1007/978-3-031-88304-0_77

Fatin, A., Muhaimin Putri, F., Fadlilah, I. N., Hanim, A. L., Faradilla, R. G., Dwiyantie, D. O., Zahroh, A., & Safitri, M. (2024). Audit Sistem Informasi Menggunakan COBIT 5 Domain DSS001 dan DSS005 (Studi Kasus Perpustakaan Upn Veteran Jawa Timur). *Jurnal Informatika Dan Teknik Elektro Terapan*, *13*(1), 2830–7062. https://doi.org/10.23960/JITET.V13I1.5886

Firnaldo, F., Sholihah, U., & Yunita, S. (2023). Perancangan Enterprise Architecture Pada PT. Trisatya Cipta Hutama Menggunakan TOGAF. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(3), 959–970. https://doi.org/10.29100/JIPI.V8I3.3998

Garrett, R. K., Anderson, S., Baron, N. T., & Moreland, J. D. (2011). Managing the interstitials, a System of Systems framework suited for the Ballistic Missile Defense System. *Systems Engineering*, *14*(1), 87–109. https://doi.org/10.1002/SYS.20173

Gaudêncio, B., Ferraz, J., Martins, P., Váz, P., Silva, J., Abbasi, M., & Cardoso, F. (2024). A Comparison of DoDAF, TOGAF, and FEAF: Architectural Frameworks for Effective Systems Design. *International Conference on Disruptive Technologies, Tech Ethics and Artificial Intelligence*, 363–371. https://doi.org/10.1007/978-3-031-66635-3_31

Ghalib, Y. W., Gilang, E. F., Zumi M, Abdhe F, Nanda A, Serly D A, & Zurkiyah A. (2024). Analisis Perkembangan Keamanan Siber Dampak Dari Kebocoran Data Pusat Data Nasional Sementara 2 Surabaya. *JISCO : Journal of Information System and Computing*, *2*(1), 27–41. https://doi.org/10.30631/JISCO.V2I1.100

Ghozie Afiansyah, H., Annisa, N., & Febriyani, K. (2023). Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022. *Info Kripto*, *17*(3). https://doi.org/10.56706/IK.V17I3.81

Hadiati, S., & Pramuda, A. (2024). Concept Attaiment Model Based on Traditional Technology Organizers for Strengthening Global Science Literacy and Creative Character. *Jurnal Penelitian Pendidikan IPA*, *10*(6), 2927–2934. https://doi.org/10.29303/JPPIPA.V10I6.7270

Hambali, H. (2021). Penerapan Domain Monitor and Evaluate Framework COBIT 4.1 Dalam Pelaksanaan Audit Sistem Informasi. *Journal of Science and Social Research*, *4*(2), 205–211. https://doi.org/10.54314/JSSR.V4I2.608

Hidayat, R. S., Indrajit, R. E., & Dazki, E.. (2024). TOGAF's Approach in Developing an Enterprise Architecture for the Information Technology Security Industry. *Journal La Multiapp*, *5*(5), 630–645. https://doi.org/10.37899/journallamultiapp.v5i5.1524

Hilmi, M. A. Al, Puspaningrum, A., Darsih, Siahaan, D. O., Samosir, H. S., & Rahma, A. S. (2023). Research Trends, Detection Methods, Practices, and Challenges in Code Smell: SLR. *IEEE Access*, *11*, 129536–129551. https://doi.org/10.1109/ACCESS.2023.3334258

Hutagalung, N. M., Sudianto, Y., Kusumawati, A., & Fajria, A. (2024). Designing an Information System Architecture for the East Java Community Eye Hospital Pharmacy using TOGAF ADM 9.2 Approach. *Sistemasi*, *14*(1), 406–420. https://doi.org/10.32520/STMSI.V14I1.4932

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th Editio). International Telecommunication Union. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Isdiyanto, B. R. (2024). Analisis Sistem Pertahanan Udara Indonesia dalam Menghadapi Ancaman Keamanan Indo Pasifik Tahun 2022 – 2024. *Diplomacy and Global Security Journal : Jurnal Mahasiswa Magister Hubungan Internasional*, *2*(2), 1065–1071. https://doi.org/10.36859/DGSJ.V2I2.4576

Jardim, R., dos Santos, M., Neto, E., Muradas, F. M., Santiago, B., & Moreira, M. (2022). Design of a framework of military defense system for governance of geoinformation. *Procedia Computer Science*, *199*, 174–181. https://doi.org/10.1016/J.PROCS.2022.01.022

Juliana, J., Alamsyah, A., & Halim, S. (2024). Analysis of Electronic Medical Records Data Security: Case Study in Citra Husada Sigli Hospital. *Jurnal Penelitian Pendidikan IPA*, *11*(6), 773–782. https://doi.org/10.29303/JPPIPA.V11I6.11081

Julianto, A. S., Hikmah, I. R., & Yasa, R. N. (2024). Cyber-Risk Management Menggunakan NIST Cyber Security Framework (CSF) dan Cobit 2019 pada Instansi XYZ. *Info Kripto*, *18*(2), 41–47. https://doi.org/10.56706/IK.V18I2.99

Juma, A. H., Arman, A. A., & Hidayat, F. (2023). Cybersecurity Assessment Framework: A Systematic Review. *10th International Conference on ICT for Smart Society, ICISS 2023 - Proceeding*. https://doi.org/10.1109/ICISS59129.2023.10291832

Kartika, A. D., & Yolanda, D. (2024). Pengembangan Arsitektur Bisnis Berbasis TOGAF untuk Penjaminan Mutu Proses Pembelajaran di Perguruan Tinggi (Studi Kasus Fakultas Teknologi Informasi, Universitas Andalas). *Didaktika: Jurnal Kependidikan*, *14*(2), 2131–2148. https://doi.org/10.58230/27454312.1970

Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, *22*(4), 1005–1027. https://doi.org/10.1007/S10207-023-00680-4/TABLES/1

Khusumawati, T. (2024). Pendekatan Geopolitik Terhadap Kekuatan Strategis Keamanan Nasional Indonesia dalam Menyikapi Rivalitas AS–China di Asia Tenggara: Penelitian. *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan*, *4*(1), 3357–3362. https://doi.org/10.31004/JERKIN.V4I1.2130

Konnon, M. A., Lodonou, N., Gaffan, R. H., & Ezin, E. (2023). An Extended Layered Information Security Architecture (ELISA) for e-Government in Developing Countries. *International Journal of Engineering Trends and Technology*, *71*(1), 109–123. https://doi.org/10.14445/22315381/IJETT-V71I1P210

Kshetri, N. (2005). Information and communications technologies, strategic asymmetry and national security. *Journal of International Management*, *11*(4), 563–580. https://doi.org/10.1016/J.INTMAN.2005.09.010

Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, *2*(1), 9–16. https://doi.org/10.47776/ALWASATH.V2I1.127

Lee, J. Y., Syn, S. Y., & Kim, S. (2024). Global research trends in research data management: A bibliometrics approach. *Journal of Librarianship and Information Science*, *57*(3), 719–732. https://doi.org/10.1177/09610006241239083;page:string:article/chapter

Lestari, M., Puspita, M. E., Wijaya, A. F., & Vicky. (2024). Model Tata Kelola TI Terintegrasi untuk Keamanan Informasi di Sektor Fintech. *Jurnal Teknologi Dan Manajemen Industri Terapan*, *4*(3), 766–776. https://doi.org/10.55826/JTMIT.V4I3.943

Li, W., Wang, Y., Jia, L., Peng, S., & He, R. (2024). Battlefield target intelligence system architecture modeling and system optimization. *Journal of Systems Engineering and Electronics*, *35*(5), 1190–1210. https://doi.org/10.23919/JSEE.2024.000114

Liebetrau, T. (2022). Cyber conflict short of war: a European strategic vacuum. *European Security*, *31*(4), 497–516. https://doi.org/10.1080/09662839.2022.2031991

Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. N. (2024). Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors*, *25*(15), 4545. https://doi.org/10.3390/s25154545

Marvin Immanuel, J., Rahmadewi, R., & Saragih, Y. (2024). IoT-based Facelook and Fingerprint Safe Security System. *Jurnal Penelitian Pendidikan IPA*, *10*(2), 500–505. https://doi.org/10.29303/JPPIPA.V10I2.6832

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers and Security*, *144*(June), 103964. https://doi.org/10.1016/j.cose.2024.103964

Mulyana, R. B., Riyadi, A. R., & Dhaipullah, D. (2024). Enterprise Architecture Dalam Transformasi Digital Perbankan: Studi Literatur Sistematis Menggunakan Kerangka Kerja TOGAF ADM. *Jurnal Ilmu Komputer (JILKOMP)*, *1*(1), 1–12. Retrieved from https://jurnal.or.id/index.php/jilkomp/article/view/1

Mustopo, A., Ramsi, O., & Gultom, R. A. G. (2024). Air Defense Transformation: Strategy in the Context of Multi-Domain Operations. *Formosa Journal of Applied Sciences*, *4*(7), 2081–2092. https://doi.org/10.55927/FJAS.V4I7.237

Nasiri, A. (2023). Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, *9*(1), 34–41. https://doi.org/10.34010/JTK3TI.V9I1.9672

Nezameslami, R., Nezameslami, A., Mehdikhani, B., Mosavi-Jarrahi, A., Shahbazi, A., Rahmani, A., Masoudi, A., Yeganegi, M., Akhondzardaini, R., Bahrami, M., Aghili, K., & Neamatzadeh, H. (2024). Adapting PRISMA Guidelines to Enhance Reporting Quality in Genetic Association Studies: A Framework Proposal. *Asian Pacific Journal of Cancer Prevention*, *26*(5), 1641–1651. https://doi.org/10.31557/APJCP.2025.26.5.1641

Noor, A. Z. M., Gernowo, R., & Nurhayati, O. D. (2023). Data Augmentation for Hoax Detection through the Method of Convolutional Neural Network in Indonesian News. *Jurnal Penelitian Pendidikan IPA*, *9*(7), 5078–5084. https://doi.org/10.29303/JPPIPA.V9I7.4214

Nugraha, F., & Hendrik, B. (2024). Perbandingan Framework COBIT2019 dan TOGAF dalam Manajemen Keamanan Informasi. *Journal of Education Research*, *6*(2), 462–467. https://doi.org/10.37985/JER.V6I2.2156

Pandey, D. K., & Kumar, R. (2023). Russia-Ukraine War and the global tourism sector: A 13-day tale. *Current Issues in Tourism*, *26*(5), 692–700. https://doi.org/10.1080/13683500.2022.2081789

Parums, D. V. (2021). Editorial: Review Articles, Systematic Reviews, Meta-Analysis, and the Updated Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 Guidelines. *Medical Science Monitor : International Medical Journal of Experimental and Clinical Research*, *27*, e934475--1. https://doi.org/10.12659/MSM.934475

Pemerintah Republik Indonesia. (2002). *Undang-undang (UU) Nomor 3 Tahun 2002 tentang Pertahanan Negara*. Pemerintah Republik Indonesia. Retrieved from https://peraturan.bpk.go.id/Details/44421/uu-no-3-tahun-2002

Perwej, Y., Syed, P., Abbas, Q., Dixit, J. P., Nikhat Akhtar, D., & Jaiswal, A. K. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/IJSRM/V9I12.EC04

Proudfoot, J. G., Cram, W. A., & Madnick, S. (2024). Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, *34*(3), 436–459. https://doi.org/10.1080/0960085X.2024.2345867

Putra, D., Mutiara, D., Nugraheni, K., & Suseno, J. E. (2024). Information Technology Risk-based Enterprise Architecture Design for Training Systems: Integration of COBIT 2019 and TOGAF ADM. *JST (Jurnal Sains Dan Teknologi)*, *14*(1), 35–46. https://doi.org/10.23887/JSTUNDIKSHA.V14I1.93498

Putra, K. R., & Anggreani, F. (2022). Perancangan Arsitektur Enterprise Pada Instansi Pemerintahan: Systematic Literature Review. *Computing and Education Technology Journal*, *2*(0), 10–25. https://doi.org/10.20527/CETJ.V2I0.5293

Ramadhanty, N. (2024). Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam

Menghadapi Ancaman Risiko Siber. *Journal of Indonesian Management*, *4*(4). https://doi.org/10.53697/JIM.V4I4.1973

Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2024). Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Information Security Journal*, *33*(1), 54–72. https://doi.org/10.1080/19393555.2023.2195577

Safarudin, M. S. (2021). Analisis dan Desain Sistem Informasi Sumber Daya Manusia pada PT.DEF Metode TOGAF ADM (The Open Group Architecture Process Architecture Development Method). *Zona Teknik: Jurnal Ilmiah*, *15*(2), 16–26. https://doi.org/10.37776/ZT.V15I2.813

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability 2023, Vol. 15, Page 13369*, *15*(18), 13369. https://doi.org/10.3390/SU151813369

Septipalan, M. L., Widiartha, I. B. K., Zubaidi, A., & Taufik, M. (2024). Integrated Notification System for Smart Parking Security Using Bot Telegram. *Jurnal Penelitian Pendidikan IPA*, *10*(5), 2679–2686. https://doi.org/10.29303/jppipa.v10i5.7447

Seyboth, C., & Beckmann, H. (2024). Erstellung von Enterprise Architectures mit COBIT, TOGAF und ArchiMate. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *352*, 1639–1648. https://doi.org/10.18420/inf2024_142

Siregar, A. A., Simanungkalit, E., & Nasrudin. (2024). Telegram-Based Earthquake Early Warning. *Jurnal Penelitian Pendidikan IPA*, *11*(5), 85–94. https://doi.org/10.29303/jppipa.v11i5.11080

Siroli, G. P. (2018). Considerations on the Cyber Domain as the New Worldwide Battlefield. *The International Spectator*, *53*(2), 111–123. https://doi.org/10.1080/03932729.2018.1453583

Steingartner, W., Galinec, D., Kozina, A., Su, C., Cha, S.-C., & Tu, F. (2021). Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. *Symmetry 2021, Vol. 13, Page 597*, *13*(4), 597. https://doi.org/10.3390/SYM13040597

Stephanie, Darianty, R., Ayumi, & Fayola, A. (2024). Tinjauan Literatur terhadap Persiapan dan Tantangan Implementasi Enterprise Architecture di Pemerintahan. *JDMIS: Journal of Data Mining and Information Systems*, *2*(2), 97–104. https://doi.org/10.54259/JDMIS.V2I2.2958

Tristantie, N., & Dwi Nitami, D. (2024). Critical Thinking Implied to Fashion Research Competencies. *Jurnal Penelitian Pendidikan IPA*, *11*(2), 685–690. https://doi.org/10.29303/JPPIPA.V11I2.10185

Vernandy, F., & Herdi, T. (2023). Enterprise Architecture untuk Travel Haji dan Umroh Berdasarkan The Open Group Architectur Framework. *Jutisi : Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *12*(3), 922–933. https://doi.org/10.35889/JUTISI.V12I3.1337

Vors, O., & Bourcier, L. A. (2022). Synthesis and literature review of different mixed methods designs in pedagogical research in physical education. *Physical Education and Sport Pedagogy*, *27*(2), 117–129. https://doi.org/10.1080/17408989.2021.1999920

Wang, S., Li, J., Zhao, J., & Yang, J. (2024). Research on Architecture Design and Description Methods Based on DoDAF. *Lecture Notes in Electrical Engineering*, *1187 LNEE*, 366–372. https://doi.org/10.1007/978-981-97-2120-7_45

Wibisono, I. (2023). The Algorithm of Digital Branding of Presidential Candidacy on Instagram: Duty of Computer Technology. *Jurnal Penelitian Pendidikan IPA*, *9*(SpecialIssue), 379–384. https://doi.org/10.29303/jppipa.v9ispecialissue.6270

Willett, M. (2023). The Cyber Dimension of the Russia-Ukraine War. In *Survival: October - November 2022* (1st Editio, pp. 7–26). Routledge. https://doi.org/10.4324/9781003422211-1

Yasmin, T. S., & Yulianto, T. (2024). Enhancing Email Security Against Phishing Attacks Through User Behavior Analysis and Data Loss Prevention (DLP). *Jurnal Penelitian Pendidikan IPA*, *11*(4), 590–600. https://doi.org/10.29303/JPPIPA.V11I4.10781

Yolanda, S., Hendra, H., Hita, H., & Ginting, T. W. (2023). Analisis Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 Domain BAI03 (Studi Kasus: PT. Berlian Tangguh Sejahtera). *Jurnal Sifo Mikroskil*, *24*(2), 173–186. https://doi.org/10.55601/JSM.V24I2.1035

Younas, A., Inayat, S., & Sundus, A. (2021). Joint displays for qualitative-quantitative synthesis in mixed methods reviews. *Research Methods in Medicine & Health Sciences*, *2*(3), 91–101. https://doi.org/10.1177/2632084320984374