IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 February 2023, accepted 19 February 2023, date of publication 24 February 2023, date of current version 1 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3248622

RESEARCH ARTICLE

A Comprehensive Framework for Migrating to Zero Trust Architecture

PACHAREE PHIAYURA AND SONGPON TEERAKANOK
Faculty of Information and Communication Technology, Mahidol University, Nakhon Pathom 73170, Thailand
Corresponding author: Pacharee Phiayura (pacharee.phi@student.mahidol.ac.th)

This work was supported in part by the Faculty of Information and Communication Technology, Mahidol University.

ABSTRACT Migrating to Zero Trust Architecture (ZTA) is a strategic approach to strengthen the enterprise's security postures. The shift to ZTA requires changes across the enterprise which can be challenging to achieve. Utilizing an effective framework for migrating from the old security architecture to ZTA can help ensure smooth transitioning to the Zero Trust journey. In previous research, the effective frameworks and processes for migrating to ZTA have not been achieved in an integrated and comprehensive manner. This study introduces a comprehensive framework for migrating to ZTA. The methodology of this study is to analyze and synthesize published studies relating to ZTA migration. The findings from existing knowledge construct a process-driven for the ZTA migration. In addition, the study addresses migration challenges and gaps in existing ZTA migration approaches. As a result, a comprehensive Zero Trust migration framework is developed to construct streamlined processes. The proposed framework can be used as a reference model for effective transitioning to ZTA.

INDEX TERMS Zero trust, zero trust architecture, ZTA, zero trust migration, zero trust challenge.

I. INTRODUCTION

Nowadays, the border of the perimeter of an enterprise network security is widened due to the proliferation of cloud technologies, IoT devices, and remote workforce. As a result, the traditional perimeter-based method will become obsolete and less efficient in protecting the enterprise from cyber threats. Hence, enterprises are driven to adopt effective security strategies to improve security visibility and controls to prevent the risks and challenges of data and revenue losses.

Zero Trust Architecture (ZTA) is a security strategy developed to handle cyber threats and security breach risks. Zero Trust (ZT) assumes that there is no trusted perimeter. Users and devices only receive the least privileged access. In the Zero Trust environment, continuous verification and authorization are required for users when accessing enterprise resources [1]. Thus, ZTA can help improve visibility and analytics across the enterprise network. 83% of 1,300 security and risk specialists that responded to an Ericom Software survey agreed that Zero Trust is an effective security strategy. They plan to implement Zero Trust solutions in their enterprises [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

However, transitioning to ZTA is challenging and can be a long journey. The enterprise may encounter many challenges and barriers when migrating to a Zero Trust ecosystem. One of the challenges is the lack of industry standards and concrete frameworks for effectively implementing ZTA in enterprises. In addition, migrating to ZTA requires IT system compatibility and interoperability. Therefore, before migrating to ZTA, it is crucial to understand infrastructure requirements completely.

This research aims to study and examine existing knowledge and techniques of the ZTA migration by applying a systematic review to analyze and synthesize the published studies relating to ZTA migration. The analysis creates a process-driven framework for the migration to ZTA. Furthermore, this study argues the need for a comprehensive ZTA migration by identifying what is lacking in other frameworks. As a result, an appropriate Zero Trust migration framework is developed to establish effective processes that serve as a reference model to support a smooth transition to Zero Trust Architecture.

This paper is organized as follows. Firstly, the background of ZTA migration and challenges are described in section II. Secondly, section III describes research methodology and a comprehensive framework for migrating to ZTA is discussed

in section IV. Next, section V shows framework evaluation and section VI provides discussion of this study. Section VII describes limitations and section VIII discusses potential future work. Finally, we conclude this paper in section IX.

II. ZTA MIGRATION AND CHALLENGES

This section explains some migration methods from many studies that we obtain for the analysis. Additionally, it describes common challenges and roadblocks that hinder the success of implementing ZTA in enterprises.

A. ZTA MIGRATION

The ZTA migration is an essential security strategy that many enterprises plan to adopt to help improve security and protect enterprises from cyber-attacks and data breaches. In this study, we obtained relevant published studies regarding the ZTA migration from many sources, namely business, academic and governmental organizations. These studies provide knowledge and methods to migrate to ZTA in their practices.

According to NIST SP 800-207 [3], it is recommended to utilize an incremental approach by having a pilot program. An enterprise identifies the first group of candidates and extends the migration to subsequent phases. Furthermore, this study emphasizes the importance of identifying assets, business workflows, and risk management. Similarly, the technical guidance by CISCO focuses on establishing user trust and device visibility. Their ZTA migration concerns three main perspectives: strategic, managerial, and operational [4]. However, there is a lack of details on migration methods and techniques to migrate to ZTA.

The ZTA migration of Google BeyondCorp concentrates on technical migration methods by showing the implementation of devices, users, and network management in the ZT environment. The migration is undertaken in repetitive processes from a small pilot and increases the rollout for candidates over time [5], [6]. In contrast, Microsoft concerns with managerial methods for the ZTA migration by having all stakeholders buy in and define the scope of implementation. They divide the implementation of the ZTA into different components, namely identity, device, access, and service. Furthermore, they define the criteria of ZTA implementation measurements [7], [8].

Many ZTA implementation studies suggest the main steps for migrating to ZTA. The initial step is to identify the protecting surface, particularly data, assets, applications and services. After that, the protecting surface will be mapped to transaction flows. Moreover, the network needs to be architecturally designed to be micro-segmentation. Then, an enterprise creates and enforces the Zero Trust policies. The final step focuses on monitoring and maintaining the ZTA to securely and efficiently protect the enterprise [9], [10], [11], [12]. However, most studies lack theoretical support for their migration techniques. Furthermore, some studies mainly focus on migration's technical or managerial perspectives. There is also a lack of dynamic and comprehensive frameworks or processes to depict how to smoothly and efficiently migrate to ZTA.

B. ZTA MIGRATION CHALLENGES

This section shows common challenges when migrating to ZTA based on the analysis and synthesis of obtained studies. There are eleven challenges that discuss technical and managerial issues on ZTA migration.

1) VENDOR LOCK-IN

This issue has occurred in other technologies, such as IoT and cloud technology. Some cloud service providers, for instance, offer discounts and special deals to attract new customers to join their services and discourage users from switching to other cloud services. In addition, cloud service providers may prevent users from leaving by imposing legal restrictions, technical barriers, or additional fees [13].

2) LACK OF INDUSTRY STANDARD

Currently, no industry standard provides concrete guidance on how to implement ZTA in the enterprise. Consequently, it is challenging to have a complete picture of whether the ZTA has successfully implemented it in their enterprises [14]. Additionally, some ZT platform components require standardization. For example, the policy decision point (PDP) involves the collection of information exchange from several sources. However, this system lacks uniform standards for data exchange [13].

3) USER DISRUPTIONS DURING MIGRATION

The enterprise may experience technical issues and user disruption during each migration phase. The ZTA migration aims to replace users from the old system with the new IT environment [13]. Therefore, the enterprise may need to prepare to provide remediation for users when they are experiencing errors or difficulties during the ZTA migration.

4) LEGACY SYSTEMS

Migrating to ZTA may cause some defects to the old systems, applications, or infrastructure. As a result, it might create a situation where more resources must be carefully managed than initially planned. In addition, if these systems require redesign or modification to support ZTA, it may require more cost and time to facilitate this ZTA transition [10]. For instance, many enterprises may currently use legacy identity systems that have been using many years, such as password-based user authentication. However, using password-based verification has been shown to be inefficient [14]. Therefore, an enterprise should determine whether to upgrade or replace the legacy technologies to work efficiently in the ZT environment.

5) ZTA SERVICE CONTROLS

The ZT platform consists of several intelligently supported systems to make an appropriate decision to grant user's

access. These systems require accurate and reliable trust levels and trust algorithms. However, determining an appropriate level of trust can be challenging to ensure that a trust level is not too high or low [13]. For example, too high trust levels may block users when attempting to access the service. In contrast, the level of trust should not be too low; otherwise, security may be compromised. Furthermore, as security information comes from many sources and systems, an enterprise must ensure that supported systems in the ZT platform do not work in isolation [15]. Having isolated security tools may prevent the ZT platform's efficient and accurate visibility and analytics.

6) INTEGRATION ISSUES

Migrating to ZTA is a complex adjustment and configuration. First, an enterprise must understand infrastructure requirements and ZT-supported systems to support security functions. The ZT platform may comprise many services across multiple providers. [17]. For example, the ZT platform should be able to integrate with a software-defined network (SDN), Secure Access Service Edge (SASE), or cloud-based security. It should also interact with any network, such as broadband, 5G, or LTE [19]. Making them serve as a single control pane may be difficult and cause integration concerns.

7) ZERO TRUST POLICIES

It can be challenging for an enterprise to develop valid, consistent, comprehensive ZT policies to support ZT decisions. The ZT policies must be up-to-date with the context changes and access restrictions [18]. Many enterprises use simple access control policies, such as RBAC or ABAC. It is essential that the policy rules must be based on the least privilege principles with dynamic trust-based access control that users only have access to information or resources they need [19]. In addition, The ZT policies should not be too complex. However, developing ZT policies to accommodate the changes is challenging, mainly due to time limitations.

8) DISCOVERY RESOURCES

Discovering all resources to accommodate the ZTA migration requires time and effort to gather and analyze data. For large and complex organizations, it can be challenging when enterprises have inadequate monitoring of their IT environments. Moreover, there are issues with shadow IT or unmanaged devices. These issues may cause difficulty when performing resource discovery because the enterprise may not completely control these devices [13].

9) POLITICAL RESISTANCE

The migration team may encounter political resistance to change when introducing new systems or technologies to the enterprise. For example, employees or individuals resist change due to technical bias in security systems or architecture [20]. Therefore, when migrating to ZTA, the migration team should consider managing political resistance in the organization.

10) REGULATORY COMPLIANCE

Industrial or supervisory authorities regulate many enterprises. As a result, specific data or systems of the enterprises must comply with regulatory requirements. However, these regulatory bodies may lack behind innovative technology solutions [20]. Consequently, it is challenging for enterprises to adopt new technologies and satisfy regulatory requirements.

11) ANALYSIS PARALYSIS

An enterprise should thoroughly understand its technology and architecture requirements before implementing the ZTA. Moreover, it is essential to identify the scope and understand risks as these factors may delay the actions of the ZTA implementation [20]. However, inadequate ZTA research and analysis can cause difficulty in the zero-trust journey of the enterprise.

III. RESEARCH METHODOLOGY

This study defines research questions and uses a systematic literature review to obtain quality studies relevant to ZTA migration. Additionally, we develop our methodology to develop a proposed comprehensive ZTA migration framework as described in the following subsections.

A. RESEARCH QUESTION

The transition to ZTA can be challenging for an enterprise. Therefore, it is essential to thoughtfully implement ZTA with effective strategies and leverage appropriate technologies for the migration. In this research, we would like to answer the following questions:

1) RQ1: What are the existing Zero trust migration concepts and processes of Zero Trust Architecture?
2) RQ2: What are the Zero Trust Migration challenges, and what is lacking in other Zero Trust migration frameworks?
3) RQ3: By reflecting on other technological migration frameworks, can they help optimize and enhance a proposed zero trust migration framework?
4) RQ4: What can be an appropriate Zero Trust Migration Framework?

B. A SYSTEMATIC REVIEW

A systematic review in this study is conducted by using the PRISMA method (The Preferred Reporting Items for Systematic reviews and Meta-Analyses) to perform a literature search to identify published papers and relevant reports on the ZTA migration. The PRISMA provides a transparent method for reviewers to identify, select and synthesize studies [21].

The literature search is conducted in two parts. Firstly, we perform a literature review by searching and selecting academic peer-reviewed literature such as journals and

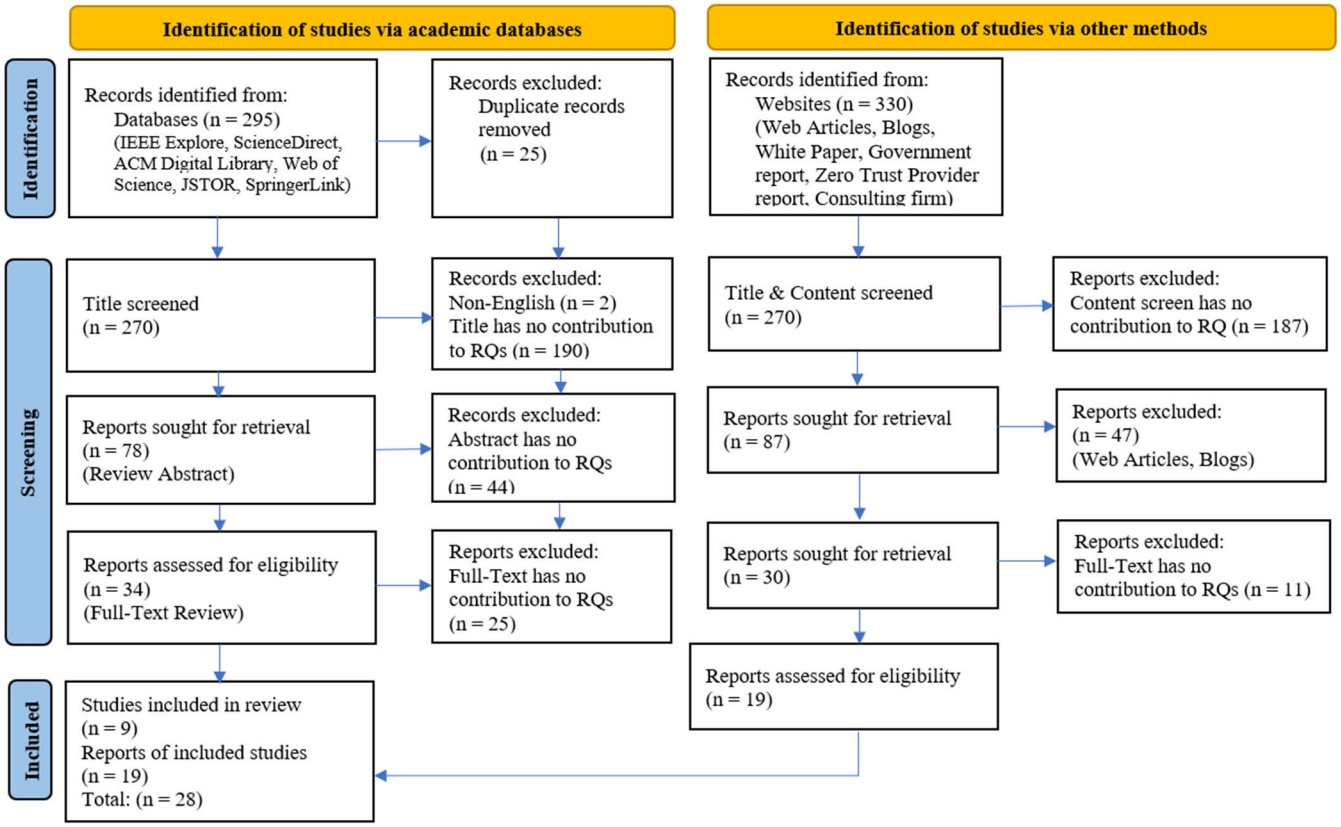

FIGURE 1. The PRISMA flowchart showing the process of selecting and obtaining the literature for our study [21].

conference papers. Secondly, we use a web search to find and select literature from credible expert sources such as government reports and white papers from Zero Trust provider reports. We then record the identification of studies used in this study by adding information to the PRISMA flowchart, as shown in Fig. 1.

1) IDENTIFICATION OF STUDIES VIA ACADEMIC DATABASE

We define the search strings "Zero Trust" and "Zero-Trust" as the terms for searching scholarly publications. We run the search term through six reputable academic databases: IEEE Explore, ScienceDirect, ACM Digital Library, Web of Science, JSTOR, and SpringerLink.

Next, we review the title of the academic articles and found 295 studies that are relevant to the ZTA concepts to perform a further screen for the review. After that, we exclude duplicate articles from other databases and eliminate articles not published in English. Then we review the abstracts of 78 publications and excluded 44 studies that did not contribute to our research questions. Finally, we perform a full-text review of 34 studies and found 9 that contribute to our analysis.

2) IDENTIFICATION OF STUDIES VIA OTHER METHODS

To include the grey literature in our analysis, we apply the guidelines by V. Garousi et al. [22]. These guidelines provide a practical process to incorporate the grey literature such as white papers, reports and ensure high quality of selected grey literature (See Appendix IX). We specify the search keywords "Zero Trust Migration," "Zero Trust Implementation," and "Zero Trust Migration white paper" to look for the ZTA migration's studies on the web.

We apply our search terms in Google Search Engine. As we scope down our search for the first 10 pages of google for each search term, we identify 330 relevant grey literature for further screening. We review title and scan the text for the search results. We exclude 187 studies that are not qualified for further screening. Then, after reviewing 87 studies, we eliminate 47 web articles and blogs since they do not offer insightful information for the ZTA migration. Next, we review 30 publications and exclude 10 studies that do not contribute to the research questions. Finally, we identify 19 high-quality reports for our analysis.

C. FRAMEWORK DEVELOPMENT METHODOLOGY

To establish a comprehensive framework for the ZTA migration, we create framework development methodology as a process to effectively develop our proposed ZTA migration framework as shown in Fig. 2. The output of each process is aimed at analyzing and improving the ZTA migration processes. The methodology of developing a ZTA migration framework comprises 5 steps as follows:

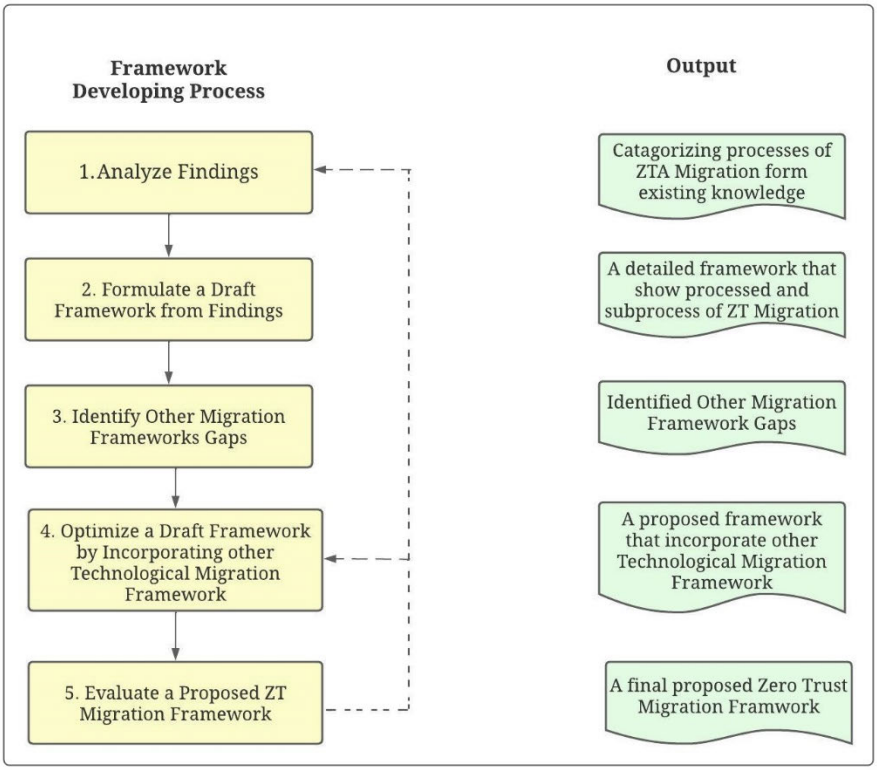

FIGURE 2. The methodology of developing a ZTA migration framework.

1) STEP 1 – ANALYZE FINDINGS

After acquiring qualified studies from a systematic review, we analyze them to understand the ZTA methods and techniques. We then classify the studies discussing similar concepts of migration into six main processes. Table 10 demonstrates details of obtained studies and categorizes the studies into processes. Additionally, Table 11 summarizes the main concepts of each obtained study (See Appendix -B, Table 10 and Table 11).

2) STEP 2 – FORMULATE A DRAFT FRAMWORK FROM FINDINGS

In this step, we formulate a draft framework from the analysis results of the previous step to gain more details regarding the methods and techniques of the migration.

3) STEP 3 – IDENTIFY OTHER FRAMEWORK GAPS

This step is to identify the gaps from other studies and determine what other frameworks are lacking in their migration processes, as shown in Table 1. The ZTA-related migration studies are given framework code and evaluate their studies against main processes defined in step 2.

4) STEP 4 – OPTIMIZE A DRAFT FRAMEWORK

We plan to optimize a draft ZTA migration framework by incorporating other technological migration methodologies, such as cloud migration and DevOps methodology. This step will help enhance a draft framework to be more effective for the ZTA migration. In this study, we utilize the DevOps methodology to optimize the proposed framework, as shown in Fig.3 and Fig. 4.

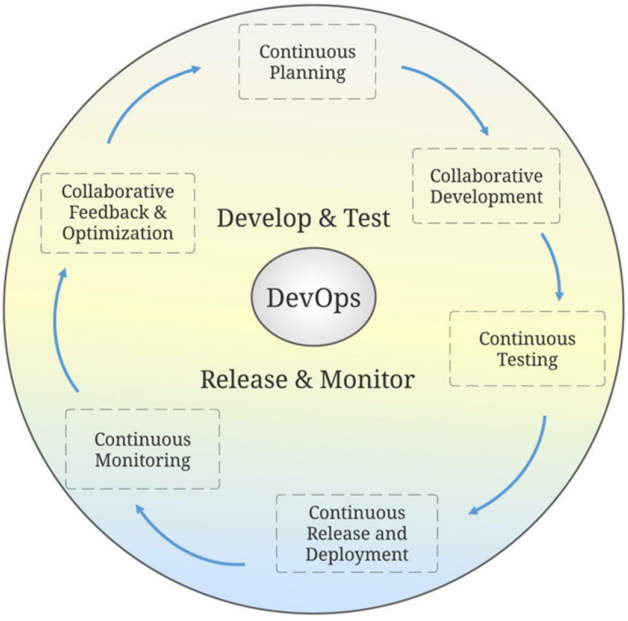

FIGURE 3. DevOps cycle.

TABLE 1. Identification of other migration framework gaps.

Framework Code	Strategize Zero Trust	Context Assessment	Architect ZTA	Zero Trust Transformations	Monitoring and Maintenance	Optimize ZTA Security
[A1]		✓			✓	
[A2]		✓	✓			
[A3]		✓				
[A4]				✓		
[A5]		✓				
[A6]			✓			
[A7]	✓					
[A8]	✓	✓		✓		
[A9]		✓	✓		✓	✓
[A10]	✓	✓	✓	✓		
[A11]	✓		✓	✓		
[A12]	✓	✓	✓		✓	
[A13]	✓		✓			✓
[A14]	✓	✓	✓	✓	✓	✓
[A15]		✓	✓		✓	✓
[A16]	✓	✓	✓			
[A17]			✓			
[A18]		✓		✓		✓
[A19]	✓		✓	✓		
[A20]	✓		✓			
[A21]			✓		✓	

5) STEP 5 – EVALUATE A PROPOSED ZTA MIGRATION FRAMEWORK

We develop evaluation criteria to evaluate a proposed ZTA migration framework (See Table 2 and Table 3). This evaluation framework is also used to evaluate other ZTA migration frameworks that we obtained for our analysis to understand the quality and effectiveness of each framework.

IV. PROPOSED FRAMEWORK

This section proposes a comprehensive framework for migrating to ZTA based on our analysis and synthesis. The importance of optimizing the proposed framework by incorporating DevOps methodology is described in sub-section A. In addition, the main processes and sub-processes of the migration are elaborated in sub-section B.

A. INCORPORATING DevOps METHODOLOGY

DevOps is a software development methodology that emphasizes collaboration, communication, continuous integration, and software quality assurance. It aims to bridge the gap between development and operations [23], [24]. Moreover, it adds a more value-driven and customer-centered approach to agile software development [23]. As DevOps intends to remove boundaries between development and operation, it helps an enterprise to achieve high service quality and stability of performance. In addition, the lead time of product delivery increases due to understanding customer needs by receiving quick customer feedback [25]. As a result, the quality and efficiency of the product will also increase.

DevOps consider the entire software development and operations life cycle, as shown in Fig. 3. The main aspects of DevOps include capabilities such as continuous planning, continuous deployment and delivery, and continuous evaluation and feedback [23], [24], [25]. Moreover, an enterprise should ensure continuous operation to avoid disrupting end users when managing software and hardware updates.

From our perspective, the DevOps paradigm and concepts can be well adapted to optimize the ZTA migration as it shares common aspects regarding the technology development and migration cycle. For example, the migration of ZTA requires a high collaboration of stakeholders. Furthermore, the migration project is undertaken in iteration and extends the migration to the phases after ensuring effective migration methods from monitoring and feedback. Therefore, incorporating DevOps concepts with the ZTA migration framework can increase effectiveness and create more value across the migration process.

B. A PROPOSED COMPREHENSIVE ZTA MIGRATION FRAMEWORK

According to the results of the synthesis and qualitative analysis of our obtained studies, we propose a comprehensive framework for migrating to ZTA. This comprehensive framework depicts the main processes and sub-processes to migrating to ZTA. It comprises six essential processes: strategize

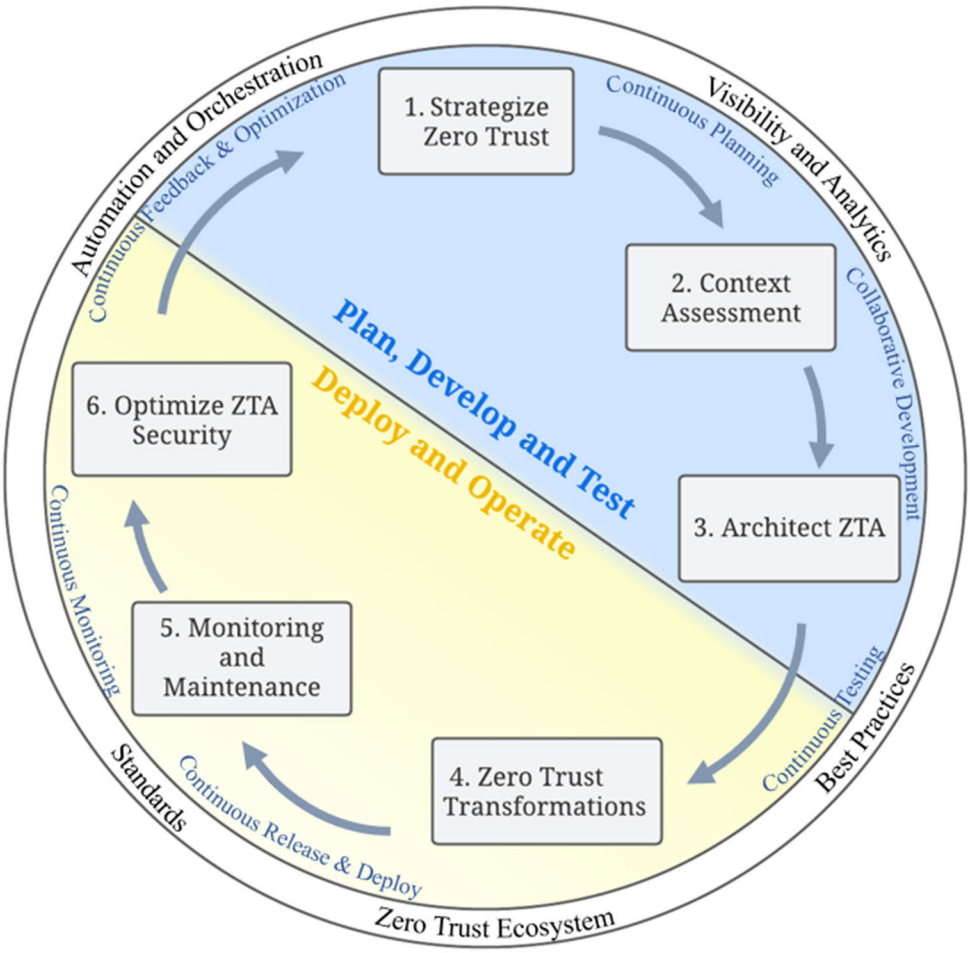

FIGURE 4. A proposed comprehensive framework for migrating to ZTA.

Zero Trust, context assessment, architect ZTA, Zero Trust transformation, monitoring and maintenance, and optimize ZTA security, as shown in Fig. 4 and 5.

A comprehensive framework for migrating to ZTA incorporates the concepts of DevOps methodology to ensure service delivery quality. In addition, the migration processes take into account the Zero Trust ecosystem in which visibility, analytics, automation, and orchestration are emphasized. Migrating to ZTA also needs to consider following best practices and standards to ensure compliance with industry standards and authoritative bodies.

There are six processes associated with sub-processes as follows.

1) PROCESS I - STRATEGIZE ZERO TRUST

The first process in migrating to ZTA is to strategize Zero Trust principles by creating Zero Trust strategies in an enterprise. Following the establishment of the strategies, key stakeholders such as top management and users must buy-in to support the decision to migrate to ZTA. In addition, Zero Trust teams, which involve implementation teams and IT decision makers, must be set up to support the transition. The outcome of this process is a master plan for Zero Trust migration which acts as a document for stakeholders to define what they want for their ZTA, as demonstrated in Fig. 6.

a: CREATE ZERO TRUST STRATEGY

The initial step in migrating to ZTA is to define vision and strategies and gain support from leadership and stakeholders [26], [27], [28]. The main objective is to ensure that stakeholders have seen common themes of the needs for moving to ZTA, such as enhancing business agility and managing complexity [8]. In addition, many enterprises use some data or systems that must be regulated or complied with regulatory requirements [20]. Therefore, an enterprise should proactively engage with external stakeholders early, such as governmental regulators, external auditors, or relevant third parties, as they may lag behind new technologies and have some concerns regarding the new Zero Trust solutions. The enterprise should collaborate or educate them to ensure they understand the enterprise's direction to migrate to ZTA.

1. Strategize Zero Trust	2. Context Assessment	3. Architect ZTA	4. Zero Trust Transformation	5. Monitoring & Maintenance	6. Optimize ZTA Security
▪ Create Zero Trust Strategy ▪ Set up Zero Trust Teams	▪ Assess the Current States ▪ Perform Resource Discovery	▪ Create a ZT Migration Plan ▪ Preparation of Device, User and Network ▪ Design Zero Trust Policies	▪ A Pilot Program to A Full Production Method ▪ Measure Implementation Success & Error Remediation	▪ Monitor ZT Ecosystem ▪ Measure Security Effectiveness	▪ Zero Trust Performance Upgrade Plan ▪ Adoption of Securities Automation and Orchestration

FIGURE 5. The main processes and sub-processes of ZTA migration.

TABLE 2. Framework evaluation – generic criteria.

Generic Criterion	Evaluation Question
Process Clarity	Does the framework provide a clear description of the suggested processes and activities?
Procedures & Supportive Techniques	Does the framework provide procedures or supportive techniques to perform each process?
Traceability	Does the framework identify the sequence of modelling or dependencies between processes?
Tailorability	Is the framework based on a one-fits-all assumption or define adaptative mechanisms for migration? Is the framework be expressed in the form of method fragments or process components?
Tool Support	Does the framework suggest or provide guidelines of the tools that support the ZTA migration process?
Scalability	Is the framework applicable to handle various migration sizes?
Formality	Does the framework provide a degree of formality on technical aspects?
Theoretical foundation	Is the framework inspired or developed based on the existing software engineering paradigms or practice?
Work-Products	What work-products are described by the framework to produce in the ZTA migration process?
Development Roles	What development roles, who are responsible for performing migration activities or any stakeholder who are involved, are defined by the framework?
Domain Applicability	What are application domains for which the framework offer?

Furthermore, an enterprise must create a master plan or a strategic plan for migrating to ZTA. This plan will help the enterprise know the environment, the capabilities, and the scope of implementation [16], [29]. It is essential to start the ZT pilot project as soon as possible, even if there is an initial limitation of scope [20]. In doing so, an enterprise can

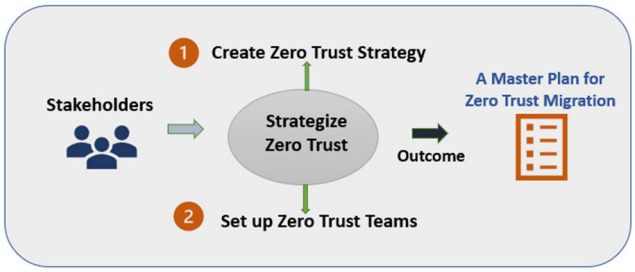

FIGURE 6. Process 1 - Strategize Zero Trust.

define what they want for their Zero Trust architecture and investigate available Zero trust solutions early.

b: SET UP ZERO TRUST TEAMS

Concerning the success of Zero Trust implementation, Zero Trust teams are essential for the smooth transition of the Zero Trust implementation projects. People involve with ZT implementation must be cross-functional team of business and IT decision makers [12], [30]. The teams can be established into two groups as follows:

- The first group acts as key decision-makers to provide direction, review the plans and support the overall project [20]. These are examples of the group of key decision-makers.
  Governance Board: Providing direction for the organization and making decisions regarding new initiatives and technologies.
  Architecture Review Board: The primary responsibility is to review current technologies and define the enterprise architecture.
  Change Management Board: The primary responsibility is to promote Zero Trust solutions in a production environment.
- The second group is a Zero Trust implementation team. The team members should be appropriately selected and be associated with these functions, namely application and data security, network and infrastructure security, and user and device identity [3], [30], [31]. It is essential that people involving with ZT implementation must be cross-functional team of business and decision makers.

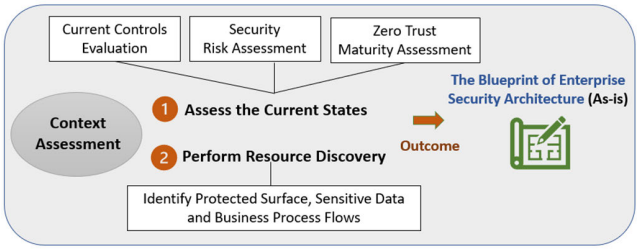

FIGURE 7. Process 2 - Context Assessment.

Furthermore, an enterprise should adequately communicate the transitioning to ZTA, especially users. The main reason is that inefficient communication can result in users' confusion and inability to provide effective remediations. The enterprise may have a communication plan or a campaign to raise awareness and inform users early to gain users' buy-in [32]. A project champion can be established to communicate and empower users to reduce barriers. The techniques that can be adopted to communicate may include in-person or town hall meetings, email, newsletters, or videos and blogs.

2) PROCESS II - CONTEXT ASSESSMENT

The second process is to conduct a context assessment, as shown in Fig. 7. This process helps an enterprise understand its current security state. To evaluate the current security state, it can be conducted through evaluating existing security controls, performing a security risk assessment, and conducting a Zero Trust maturity risk assessment. In addition, to have accurate views of resources in the enterprise, the enterprise must perform resource discovery to identify data and business process flows. The outcome of this process is to have the blueprint of enterprise security architecture. This blueprint serves as an enterprise's baseline for setting the current and desired Zero Trust maturity state.

a: ASSESS THE CURRENT STATES

This sub-process comprises three essential methods, namely 1). Evaluate current control 2). Perform Security Risk Assessment, and 3). Perform Zero Trust Maturity Assessment. These methods are important for an enterprise to have a complete picture of an enterprise's security state.

i) EVALUATE CURRENT CONTROLS

It is important to identify the enterprise's existing security capabilities. Hence, the enterprise should check and monitor that the existing security policies and regulations are compatible with the Zero Trust principle. After checking existing security controls, a gap analysis should be executed to evaluate the current state of the enterprise's security and identify security improvements [33]. Finally, as migrating to ZTA may cause problems or integration issues for the existing systems, the migration team should have an appropriate plan to evaluate the existing legacy systems and whether they can integrate and work well in the ZT environment.

ii) PERFORM SECURITY RISK ASSESSMENT

An enterprise must continually analyze and assess the risks associated with its assets and resources by identifying external and internal threats as well as actual and potential risks. Then, risk management should be planned to address the identified risks. The results of a risk assessment can be used to identify security patterns in the ZT ecosystem [3], [18]. Furthermore, performing a security risk assessment can assist the enterprise in identifying actors and assets that must be protected, as well as considering migration with low-risk processes [13]. Risk assessment also helps the enterprise design protections by minimizing access to resources based on the principle of least privilege.

iii) PERFORM ZERO TRUST MATURITY ASSESSMENT

The enterprise can better understand the current security state by conducting the Zero Trust maturity assessment. The Zero Trust maturity stage can range from the traditional stage, in which the enterprise has not started its Zero Trust journey. The next stage is the advanced stage, where the enterprise starts its Zero Trust journey and makes some progress, such as registering all devices and implementing network segmentation. The final stage is the optimal stage, where the enterprise makes huge progress in security improvements, for example, by utilizing AI intelligence to respond to access requests and detect usual activities [7]. The enterprise should set desired maturity state and identify critical success factors [26], [34]. In addition, the objectives and time frame that the enterprise plans to achieve the target ZT maturity state need to be defined.

b: PERFORM RESOURCE DISCOVERY

An enterprise must determine the protected surface and identify sensitive data, and business process flows to gain a complete view of all resources [9], [10]. However, the enterprise should understand that having complete visibility of every data flow is unnecessary before beginning the ZT implementation [3], [35]. Instead, the enterprise may consider using an observational approach to gather and analyze the data network to ensure that the system does not interrupt user productivity [20].

Before a Zero Trust deployment, an enterprise should identify protecting surfaces by surveying assets and subjects such as data, service accounts, devices, applications, services, hardware, and configuration management [13]. In addition, an enterprise must identify sensitive data and define business process flows [9]. Finally, data discovery and classification should be carried out to discover all the data processing activities. For instance, the enterprise can set up an inventory of data repositories to identify data protection levels.

The network should be segmented based on data classification [10]. Furthermore, the business process flows should be mapped with a protective surface to understand interdependencies and help develop security policies. Finally, the data

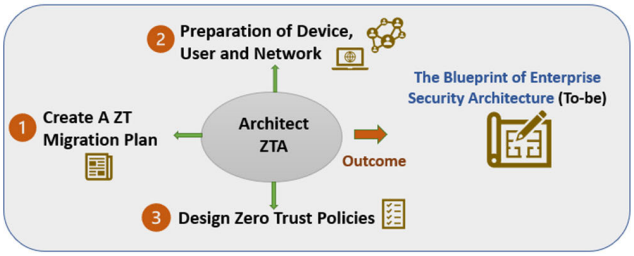

FIGURE 8. Process 3 - Architect ZTA.

and business process workflows should appropriately design who can access sensitive data in the enterprise [12].

3) PROCESS III - ARCHITECT ZTA

This process involves establishing a Zero Trust migration plan that the enterprise will use as a plan for implementing ZTA. Furthermore, an enterprise's devices, users, and network should be appropriately prepared for undertaking ZTA implementation. Additionally, the Zero Trust policies should properly be designed to provide effective security controls when granting user access to resources. As a result, the outcome of this process is establishing a target enterprise security architecture that serves as a desired state of ZTA, as illustrated in Fig. 8.

a: CREATE A ZTA MIGRATION PLAN

Before implementing ZTA in an enterprise, the available zero trust solutions and technologies should be selected appropriately [27]. The enterprise should select suitable vendors that provide zero trust solutions that meet requirements. An enterprise must have a complete understanding of the technical requirements of ZTA before buying ZT solutions from the vendors. In addition, the enterprise should consider software interoperability to avoid vendor lock-in effects. Service adaptation like QoS (quality of service) or SLA (service-level agreement) negotiations is essential to prevent the vendor lock-in issues. Moreover, an implementation plan should be developed to divide tasks and prioritize these tasks for implementation [16]. Finally, test plans and performance measurement plan for ZTA migration should be created to prepare for evaluating the success and effectiveness of the migration. The enterprise may use a use- case approach to initiate a project that aim at solving specific problems. Thus, the enterprise can see quick results by using a small team and small budget.

b: PREPARATION OF DEVICE, USER, AND NETWORK

To secure the devices, an enterprise should establish a Device Inventory Database [4]. This database is used to register devices and allows only managed devices to access an enterprise's network [5], [7]. In addition, all devices should have proper security controls and be continuously monitored to detect potential risks [35]. The main objective of registering all devices, including corporate-owned devices and personally owned devices, is to establish trust and security controls over device management.

To securely identify users, an enterprise should create a User Database to manage all users and the group of users' memberships [5]. It is also necessary to ensure the least privilege principle and have an acceptable user management approach when setting appropriate roles for users. The groups of users include business users, clients and partners of the enterprise, and IT users who can modify user access rights and other configurations. In addition, an enterprise must ensure that redundant access permissions of users are removed, and Multi-Factor Authentication (MFA) is implemented [4], [7]. In addition, an enterprise should have appropriate administrative controls, such as implementing privileged identity management (PIM) [26].

All users and devices must be allocated to the proper network to deploy an unprivileged network. The enterprise should manage the micro-segmentation of sensitive data and establish user access based on planned segmentation [10]. After understanding dependencies, the enterprise should manage and put identified assets into logical groups according to workflows and business processes. The enterprise must be aware of not an over-segmenting or under-segmenting network [36]. All traffic must pass through segmentation gateways before reaching the protected resources. Furthermore, the enterprise must ensure that network asset visibility and network security standard are implemented. The level of access for a user should be granted on a per-request basis [5].

c: DESIGN ZERO TRUST POLICIES

When creating Zero Trust policies or security policies used in the ZT environment, these policies should be appropriately created, tested, and redefined based on resources and identified transaction flows [3], [28], [36]. One of the approaches to creating the ZT policies can be based on the Kipling Method that identifies the who, what, when, where, why, and how users access the resources [11], [12]. Another approach to designing access permissions is based on different factors and the sensitivity of resources, such as data, users, devices, threats, regulatory requirements, etc. [4]. Furthermore, these policies should be ensured that they are correct, consistent, minimal, and complete [30]. For example, an enterprise needs to validate the ZT policies to ensure they are not duplicated and redundant.

4) PROCESS IV - ZERO TRUST TRANSFORMATIONS

This process begins when an enterprise selects the candidate group for migration and launches the initial deployment. Then, the selected group of candidates is migrated to the unprivileged network simulation for a certain period until the migration team can ensure qualified traffic. This group of candidates acts as the test group for the migration team to ensure the success of the migration with a low-risk strategy. After that, the migration team starts rolling out the following groups of candidates. Finally, the measurement of

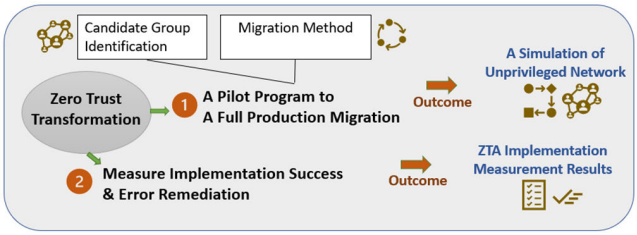

FIGURE 9. Process 4 - Zero Trust Transformations.

ZTA implementation should be undertaken to ensure that the migration has proceeded as planned, as illustrated in Fig. 9.

a: A PILOT PROGRAM TO A FULL PRODUCTION MIGRATION

i) CANDIDATE GROUP IDENTIFICATION

A Zero Trust migration project should be implemented in small-scale and manageable programs [20]. Therefore, an enterprise should identify potential groups of candidates and create the candidate workflows for the migration [3], [5]. For example, an enterprise may consider categorizing users into three groups. The first group is the test group, in which users are carefully selected to ensure low-risk migration. The following groups are external users and internal users. External users access the enterprise's resources outside the enterprise network. In contrast, internal users are users who access the enterprise's resources within the enterprise network [4].

Some users may not yet be ready to switch to the Zero Trust architecture. The migration team should provide solutions or methods for users to request temporary exemptions for the migration. These users should be listed in workflows that were not yet qualified. When the workflow is qualified, the users should be notified that they are eligible for the migration [37].

i) MIGRATION METHODS

When migrating to Zero Trust, three primary phases need to consider ensuring minor interruptions to users.

- *Phase 1: Production Pilot*

The pilot group of users for the migration should be prepared for deployment to the Zero Trust platform or the unprivileged network [5], [20]. In addition, all devices are assigned to this network. The enterprise must ensure that the applications meet the requirements of the access proxy of the Zero Trust platform and that the applications use supported protocols. All applications must run through the access proxy [34], [38]. After most applications run through the access proxy, users must be discouraged from using the VPN. The VPN should only provide to users who need to use it [5]. At this phase, the unprivileged network simulation will simulate network behavior by monitoring the network traffic of all user devices. The deployment should be deployed with security controls or in audit mode so users can be switched to the Zero Trust platform or rolled back to the old systems [21].

- *Phase 2: Validate Pilot Results*

In this phase, those users will operate by the unprivileged simulation in audit mode for a well-defined period to ensure qualified traffic. Then, users and devices having qualified traffic for a defined period can be activated and assigned to the unprivileged network [5], [18]. The results from the migration of the pilot program need to be validated to ensure that users can successfully be migrated to the Zero Trust environment or that the migration encounters any issues. If experiencing issues, the migration team should switch back to the old technologies and test the systems to ensure that the migration of the pilot program can continue as planned [18], [20].

- *Phase 3: Full Production Rollout*

The migration team continues to deploy the remaining groups of users. In this phase, the team prepares to transfer the test environment to the production operations [3], [20]. When the migration team ensures the functions, technologies, and methods, they can start to decommission the old technologies and solutions. Finally, the full enforcement of the ZT platform can be turned on [18].

b: MEASURE IMPLEMENTATION SUCCESS & ERROR REMEDIATION

The test plans and implementation metrics should be used to measure the ZTA implementation success and the effectiveness of the migrated ZTA. In addition, the enterprise should provide methods or channels to handle error remediation if there are error cases [6]. For example, an enterprise provides a self-remediate channel for users to solve simple problems or errors by following the remediation steps or manuals. In addition, the enterprise may establish self-service help. This service will answer common questions or send an automatic email to inform users about the project's timelines and how the migration may impact users [37], [38].

For complex cases, the support team needs to be ready to handle and troubleshoot and provide immediate actions for helping users. Therefore, IT staff should be educated and trained to help users affected by interruptions so that users can get back to the normal stage as quickly as possible [35]. Once the migration team gains confidence with all the functions and its Zero Trust components, the team should promote the success of the migration project to gain support and raise awareness of the Zero Trust strategy among all stakeholders [12].

5) PROCESS V - MONITORING AND MAINTENANCE

After successfully migrating to ZTA, the enterprise must monitor the ecosystem of ZTA to gain visibility of network activity. The process to monitor ZTA helps the enterprise ensure that all functions and components in ZTA work effectively or require maintenance. In addition, user experience and security effectiveness must be measured after implementing ZTA. This process aims to acquire security monitoring results and ensure that the zero trust components function well. It also reflects user productivity and security improvements gained from utilizing ZTA, as demonstrated in Fig. 10.

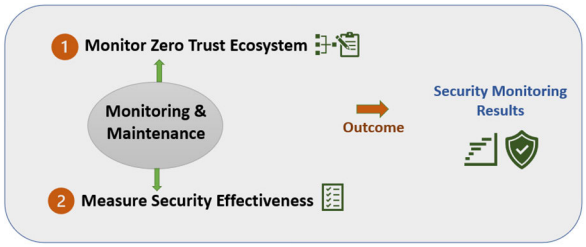

FIGURE 10. Process 5 - Monitoring and Maintenance.

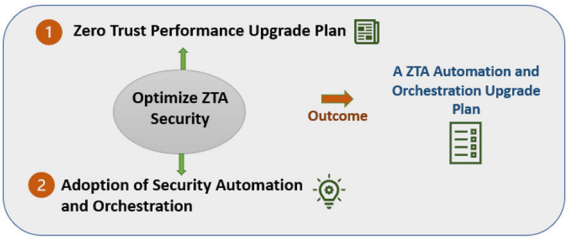

FIGURE 11. Process 6 - Optimize ZTA Security.

a: MONITOR ZERO TRUST ECOSYSTEM

An enterprise should inspect and log all traffic in the network in real-time to gain visibility of users and network activities [12], [35]. It is essential to monitor the availability of services and network components for IT operation monitoring [11]. Furthermore, an enterprise should monitor all IT infrastructure components owned by the enterprise. As for compliance monitoring, an enterprise must check and monitor security baseline, vulnerability scanning, and data breach detection.

The enterprise must continuously monitor zero trust architecture with security analytics tools [9]. As a result, the enterprise should determine whether existing security analytics tools can be utilized and ensure that those tools are appropriately placed in the logical architecture [10]. However, if the enterprise requires upgrading security analytics tools, it is essential to consider a vendor that can provide analytics solutions that work well in the ZT ecosystem.

b: MEASURE SECURITY EFFECTIVENESS

An enterprise should measure security effectiveness after successfully implementing ZTA. Regarding user experience, frictions or interruptions causing bad user experience should be measured [8]. It can be measured by checking security interruptions in user workflow. For example, when users are prompted to multifactor authentication or drop in application usage because login fails. Additionally, the enterprise may check the number of employees actively using MFA and accessing applications.

Deploying Zero Trust architecture should provide better security effectiveness. Therefore, security incidents should be reduced in quantity and incident impacts. Furthermore, Security effectiveness can be measured by the number of security incidents or percentage of time IT users spend on low-value activities such as password reset [8]. Furthermore, it can be checked by the number of manual tasks in routine workflows to investigate alerts and provide user remediations.

6) PROCESS VI - OPTIMIZE ZTA SECURITY

To optimize the security of ZTA after deploying zero-trust solutions, an enterprise should assess the effectiveness of the ZTA. After that, the enterprise should establish a plan to upgrade the capabilities of ZTA as the business must adapt and change. The desired Zero Trust capabilities should provide accurately automated actions and responses as much as possible. Hence, integrating security automation and orchestration tools can improve the capabilities of ZT by making it more automated and enabling it to detect threats more accurately, as shown in Fig. 11.

a: ZERO TRUST PERFORMANCE UPGRADE PLAN

After zero trust solutions have been fully implemented, the next stage considers upgrading its capabilities and maturity [12], [34]. This is because business and technology change over time. As a result, it is important to improve the ZT capabilities and security controls. Hence, the enterprise should consider creating a Zero Trust upgrade plan to assess the security performances and set up plans to enhance the Zero Trust performance to be more efficacious. This upgrade plan should indicate the ZT maturity stage that the enterprise aim to achieve. The most mature stage of the ZT maturity model is when the enterprise can utilize automated threat detection and responses to protect against advanced threats in a timely manner [7].

b: ADOPTION OF SECURITY AUTOMATION AND ORCHESTRATION

Zero Trust solutions should provide advanced automated actions and responses [9]. Therefore, to improve the performance of zero trust capabilities, the enterprise should assess manual security operations and procedures and consider translating those processes and procedures into technology automation [10]. In addition, security automation and orchestration should be adopted to detect security risks quickly and automatically.

The enterprise may consider integrating SOAR (security orchestration, automation, and response) or security information and event management (SIEM) tools to enhance the efficiency of security operations [28], [35]. These tools can enhance Zero Trust capabilities with a high level of automation and orchestration.

V. FRAMEWORK EVALUATION

We created an evaluation framework as criteria to evaluate other studies and a proposed ZTA migration framework, as illustrated in Fig 12. This evaluation framework will help ensure the quality, usability and effectiveness of a proposed ZTA migration framework. Each framework from other studies, including our proposed ZTA migration frame-

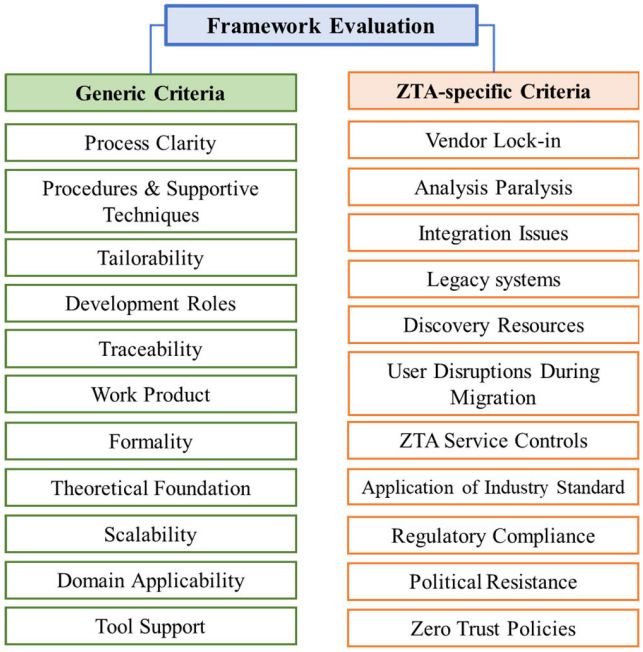

FIGURE 12. Framework evaluation criteria.

work are assessed with specific questions for each criterion (See Appendix C).

The proposed evaluation framework provides methods to evaluate the obtained studies of the ZTA migration frameworks. As a result, this helps us to understand, characterize and give answers to our research objectives. Furthermore, the evaluation framework comprises both generic and ZTA-related criteria to evaluate the ZTA migration frameworks. Therefore, the evaluation criteria provide a suitable and sufficient method to assess the ZTA migration frameworks. Moreover, the criteria are comprehensive enough that we can use them to characterize the similarity or differences among the ZTA migration frameworks.

The evaluation results of other ZTA migration frameworks and the proposed framework are assessed based on the degree of evidence found in the techniques and methods of their migration practices. Moreover, the type of criteria for evaluation includes scale, Boolean, and descriptive criteria, as depicted in Table 7 and 8.

A. GENERIC CRITERIA FOR EVALUATION

As for generic criteria for evaluation, we applied the evaluation framework of the cloud migration process by the study of M. Fahmideh et al. [39]. The generic evaluation criteria were well defined as they are synthesized by several existing frameworks regarding software engineering (See Table 2). For example, the process clarity criterion ensures that a proposed ZTA migration framework can provide a clear and comprehensive description of suggested processes. As for the theoretical foundation, it is to evaluate that the proposed framework has been developed based on the existing software engineering practices. The description of each criterion is as follows.

1) PROCESS CLARITY

Process clarity refers to specifying and clarifying the process details or activities of ZTA migration. The comprehensive and step-by-step guidance description is helpful for ZTA implementors to follow on what action should be taken.

2) PROCEDURES & SUPPORTIVE TECHNIQUES

It is essential to elaborate clear procedures and supportive techniques, such as examples to perform tasks or activities to implement ZTA. For example, IT security risk assessment, ZTA maturity assessment, and resource discovery are supportive techniques that ZTA implementers can conduct when migrating to ZTA.

3) TAILORABILITY

This criterion means the framework can be adapted or supported with various migration project situations. Moreover, it should not be based on a one-fits-all assumption. For instance, the frameworks may provide tools or techniques for customizing migration requirements or activities.

4) DEVELOPMENT ROLES

This criterion wants to assess whether the framework defines the roles, necessary skills and responsibilities of ZTA implementers. It helps us understand the required expertise in the ZTA migration process. ZTA implementers may include business leaders, IT executives, enterprise architects, and information security officers.

5) TRACABILITY

This criterion refers to the relationship in the overall process model in which each process should connect and can be traced back. In addition, the framework should provide traceability between particular processes or activities. The ZTA implementers must understand the linkage between the previous or subsequent work product throughout the lifecycle.

6) WORK PRODUCT

Work product is a crucial component of the migration lifecycle for any methodology. Therefore, a recommended framework should produce appropriate work products in each migration process. In addition, the work product can help an enterprise understand what will be delivered for the ZTA migration process.

7) FORMALITY

This criterion is used to evaluate the framework or work products that provide precise and unambiguous mechanisms for ZTA migration. Moreover, the frameworks clearly represent the relationships between work products. For example, many approaches offer low-risk migration process for migrating to ZTA.

TABLE 3. Framework evaluation – zero trust migration challenges criteria.

ZTA-Specific Criterion	Evaluation Question
Vendor Lock-in	Does the framework provide a clear description or mechanisms to manage Zero Trust vendor lock-in issues?
Analysis Paralysis	What are the strategies or techniques to analyze or perform activities of the migration process?
Integration Issues	Does the framework provide a clear description or mechanisms to manage integration issues?
Legacy systems	Does the framework provide a clear description or mechanisms to manage legacy systems issues?
Discovery Resources	Does the framework define techniques or mechanisms to discover resources?
User Disruptions During Migration	Does the framework provide a clear description or mechanisms to manage user disruptions during migration?
ZTA Service Controls	Does the framework provide clear techniques or tools to support ZTA service controls or a ZT platform?
Application of Industry Standard	Does the framework apply industry standard regarding Zero Trust migration or implementation in their migration process?
Regulatory Compliance	Does the framework take regulatory compliance into consideration in the migration process?
Political Resistance	Does the framework provide methods or techniques to manage political resistance in the migration?
Zero Trust Policies	Does the framework provide methods or techniques to establish and manage Zero Trust Policy?

8) THEORETICAL FOUNDATION

The theoretical foundation criterion aims to understand whether the ZTA migration frameworks apply theoretical knowledge or methodology, such as information technology and software engineering in their ZTA migration process.

9) SCALABILITY

Scalability refers to the applicability of the framework that can support various sizes of ZTA migration projects. Some frameworks may be suitable for large-size and complex workloads of migrations, while others might be suitable for simple and not complex migration sizes. We aim to evaluate related migration processes and activities in which the degree of interconnectivity of activities, workloads, supported tools, human resources, and applications are taken into consideration.

10) DOMAIN APPLICABILITY

This criterion aims to understand the application domain the ZTA migration framework has been established to implement. Some evaluated frameworks are designed to apply in various domains, including banking and insurance, supply chain and logistics, and healthcare organizations.

TABLE 4. Evaluation result – domain applicability criterion.

Framework Code	Domain Applicability
[A5], [A10], [A11], [A12], [A13], [A14], [A15], [A16], [A17], [A20], [A21]	The framework is generally designed to support enterprises planning to migrate to ZTA.
[A3], [A9]	Not specified
[A1]	An enterprise that has various users located in different part of the world.
[A2]	Supply Chain and Logistics
[A4]	A small-to medium-sized healthcare organization
[A6]	An enterprise that has heterogeneous environment, namely private cloud, public cloud and on-premise facilities.
[A7]	Banking and Insurance
[A8]	Transportation Services
[A19]	The federal government of the United States

TABLE 5. Evaluation Result – Work Product Criterion.

Framework Code	Work Product
[A1], [A5], [A6], [A9], [A10], [A12], [A14], [A15], [A16], [A17], [A19], [A20], [A21]	Not specified
[A2]	A checklist of security controls to integrate a ZTA
[A4]	A zero-trust network topology (micro segmentation)
[A7]	Prototype Minimal Viable Product (MVP) of portal Zero Trust framework
[A8]	Proof of Concept results and Zero trust platform production pilot
[A11]	Unprivileged network simulation
[A13]	Adaptive Security Platform
[A18]	Enterprise Application Access

TABLE 6. Evaluation result – scalability criterion.

Framework Code	Scalability
[A3], [A5], [A7], [A8], [A9], [A10], [A11], [A12], [A13], [A14], [A15], [A16], [A17], [A18], [A19], [A20], [A21]	- The framework explicitly specifies mechanisms to support various ZTA migration sizes and its scalability has been demonstrated in the ZTA migration projects. - The framework demonstrates interconnectivity of activities, workloads, supported tools, human resources, or applications to support the ZTA migration processes and activities.
[A1], [A2], [A4], [A6]	The framework does not support scalability.

11) TOOL SUPPORT

This criterion refers to supporting tools for ZTA migration that are offered or recommended by the frameworks. The tool support can be either the tools developed by the framework or existing third-party tools in the market of the ZT solutions. For example, the ZT platform, the unprivileged network simulation, SOAR, and SIEM.

TABLE 7. Framework evaluation results – generic criteria.

■ = Fully supported, ◧ = Partially supported, □ = Not supported, Yes = Criterion is met, No = Criterion is not met

Framework	Process clarity	Procedures & Supportive Techniques	Traceability	Tailorability	Tool Support	Scalability	Formality
[A1]	□	□	□	□	□	No	No
[A2]	◧	◧	◧	◧	■	No	No
[A3]	◧	◧	□	◧	◧	Yes	Yes
[A4]	◧	■	□	■	■	No	Yes
[A5]	□	◧	□	□	■	Yes	No
[A6]	■	◧	◧	◧	□	No	Yes
[A7]	□	□	□	◧	■	Yes	Yes
[A8]	■	■	◧	◧	◧	Yes	Yes
[A9]	■	◧	◧	■	□	Yes	No
[A10]	◧	□	◧	■	□	Yes	Yes
[A11]	■	■	◧	◧	■	Yes	Yes
[A12]	■	◧	◧	■	■	Yes	Yes
[A13]	◧	□	□	◧	■	Yes	Yes
[A14]	■	■	◧	◧	■	Yes	Yes
[A15]	■	■	◧	■	■	Yes	Yes
[A16]	◧	◧	◧	■	■	Yes	Yes
[A17]	◧	◧	◧	◧	◧	Yes	Yes
[A18]	■	■	◧	◧	■	Yes	Yes
[A19]	◧	◧	□	◧	□	Yes	Yes
[A20]	□	□	□	◧	◧	Yes	No
[A21]	◧	□	□	◧	◧	Yes	Yes
Fully supported	38%	29%	0	29%	52%	-	-
Partially supported	43%	43%	57%	61%	24%	-	-
Not supported	19%	28%	43%	10%	24%	-	-
A Proposed Framework	■	■	■	■	◧	Yes	Yes

B. ZTA-SPECIFIC CRITERIA FOR EVALUATION

For ZTA-specific criteria, we utilized the challenges of migrating to ZTA identified by our analysis as criteria to evaluate other studies and our proposed ZTA migration framework (See Table 3). The considerations of ZTA migration challenges as criteria of evaluation can help assess that the ZTA migration frameworks can address or consider the challenges of the migration in their practices.

VI. DISCUSSION

1) THE PRISMA SYSTEMATIC REVIEW RESULTS

Based on the systematic review, there are numerous databases to choose relevant studies of ZTA migration. The PRISMA method helps us to appropriately scope down and define inclusion and exclusion criteria to acquire related published studies.

Regarding identifying studies via academic databases, we perform our literature search in six reputable databases, namely IEEE Explore, ScienceDirect, ACM Digital Library, Web of Science, JSTOR, and SpringerLink. As a result, we found nine studies that significantly contribute to our analysis. Hence, it can be inferred that there are currently very few academic studies and scholars intensively investigating and researching ZTA migration. Therefore, migrating to ZTA is an interesting area that scholars can study extensively. As for the inclusion of the grey literature, we found numerous studies from many sources that are relevant to ZTA migration, such as blogs, web articles, and reports. Thus, it is evident that the concepts of ZTA and its migration practices are gaining popularity in the industry. However, obtaining high-quality studies is essential for our study. Therefore, we utilize the guidelines by V. Garousi et al. [22], which is advantageous to acquire high-quality grey literature such as white papers and reports for our analysis.

2) THE GAPS OF OTHER FRAMEWORKS

As is observed in Table 1, several studies focus on the processes of strategize ZTA, context assessment and architect

TABLE 8. Framework evaluation results – zero trust migration challenges criteria.

■ = Fully supported, ◧ = Partially supported, □ = Not supported

Framework	Vendor Lock-in	Analysis Paralysis	Integration Issues	Legacy systems	Discovery Resources	User Disruptions During Migration	ZTA Service Controls	Application of Industry Standard	Regulatory Compliance	Political Resistance	Zero Trust Policies
[A1]	□	□	□	□	◧	□	■	□	■	□	■
[A2]	□	□	■	□	◧	□	□	■	■	□	■
[A3]	□	■	□	□	□	□	■	■	□	□	■
[A4]	□	□	◧	■	□	□	◧	□	□	■	□
[A5]	■	□	□	□	■	■	■	■	■	□	□
[A6]	□	■	◧	□	■	□	□	□	■	■	■
[A7]	□	■	□	□	■	□	■	■	□	□	■
[A8]	□	■	◧	■	■	□	□	□	■	■	■
[A9]	□	□	■	■	■	◧	■	■	■	□	◧
[A10]	□	□	□	□	■	■	■	■	■	□	■
[A11]	□	■	■	■	■	■	■	□	□	■	■
[A12]	□	■	□	□	□	■	□	□	□	◧	□
[A13]	□	◧	◧	□	■	□	◧	□	□	◧	■
[A14]	□	■	■	◧	■	□	■	□	□	□	■
[A15]	□	■	■	□	■	□	■	■	■	□	■
[A16]	◧	■	■	□	■	□	■	□	■	□	■
[A17]	□	■	□	□	□	□	■	□	□	□	■
[A18]	□	■	■	□	□	■	■	□	□	□	□
[A19]	■	■	■	□	■	□	□	■	■	■	■
[A20]	□	□	□	□	■	□	□	□	◧	□	■
[A21]	□	◧	◧	◧	□	□	■	□	□	◧	■
Fully supported	10%	57%	38%	19%	62%	24%	62%	38%	47.5%	24%	76%
Partially supported	5%	10%	24%	10%	10%	5%	10%	0	5%	14%	5%
Not supported	85%	33%	38%	71%	28%	71%	28%	62%	47.5%	62%	19%
A Proposed Framework	◧	■	◧	◧	■	■	◧	◧	◧	■	■

ZTA in their migration practices. These processes are essential as they are the core processes of establishing ZTA migration. An enterprise needs to have strategies to migrate to ZTA and know the current state and gain visibility of resources before migrating to ZTA.

Moreover, the enterprise should thoughtfully design and architect ZTA. This process can help the enterprise design suitable implementation plans for the target architecture. Later, an enterprise starts to migrate the candidate group with a low-risk migration strategy. In addition, it can be seen that the processes of zero trust transformations, monitoring and maintenance, and optimize ZTA security is not the main focus points of many studies. However, to migrate successfully to ZTA, the enterprise should consider comprehensive migration processes to ensure a smooth transition to ZTA.

3) THE EVALUATION RESULTS OF OTHER FRAMEWORKS

As for framework evaluation results of generic criteria (See Table 7), it is noticeable that other studies explicitly lack specifying traceability or dependencies in their primary migration process. However, only some activities with some traceability or dependencies are partially identified. In addition, most frameworks provide customization of some process components.

For instance, the studies [S5] and [S10] include a risk assessment process to evaluate the current state assessment. Furthermore, the study [S20] and [S28] recommend establishing ZT policies based on the Kipling method. However, it is observed that many frameworks provide the tool support for migration. For example, [S2] uses the Software Bill of Materials (SBOM) to build their ZT solution. [S4] provides

TABLE 9. Quality assessment checklist of grey literature for software engineering [22].

Criteria	Questions
Authority of the producer	• Is the publishing organization reputable? • Is an individual author associated with a reputable organization? • Has the author published other work in the field? • Does the author have expertise in the area?
Methodology	• Does the source have a clearly stated aim? • Does the source have a stated methodology? • Is the source supported by authoritative, contemporary references? • Are any limits clearly stated? • Does the work cover a specific question? • Does the work refer to a particular population or case?
Objectivity	• Does the work seem to be balanced in presentation? • Is the statement in the sources as objective as possible? Or, is the statement a subjective opinion? • Is there vested interest? E.g., a tool comparison by authors that are working for particular tool vendor • Are the conclusions supported by the data?
Date	• Does the item have a clearly stated date?
Position w.r.t. related sources	• Have key related GL or formal sources been linked to / discussed?
Novelty	• Does it enrich or add something unique to the research? • Does it strengthen or refute a current position?
Impact	• Normalize all the following impact metrics into a single aggregated impact metric (when data are available): Number of citations, Number of backlinks, Number of social media shares (the so-called "alt metrics"), Number of comments posted for a specific online entry like a blog post or a video, Number of page or paper views
Outlet type	• 1st tier GL (measure=1): High outlet control/ High credibility: Books, magazines, theses, government reports, white papers

ZT network topology tool support. Moreover, [S11], [S19], and [S25] develop ZT security platforms as tools to facilitate ZTA migration.

Regarding the domain applicability criterion (See Table 4), most frameworks are generally established to assist enterprise planning in implementing ZTA. Some frameworks are specifically designed to support particular domains such as supply chain and logistics, banking and insurance, and healthcare organization.

As for the work-product criterion, few obtained studies produce work products relating to their ZTA migration frameworks. Many frameworks lack demonstrating ZTA-related work products in their migration approaches, as shown in Table 5.

For the scalability criterion (See Table 6), it is evident that many obtained studies can support the scalability of their ZTA migration projects as they specify mechanisms to handle various migration project sizes. In addition, most frameworks identify the interconnectivity of activities, workloads, supported tools, human resources, or applications.

According to framework evaluation of ZTA-related criteria (See Table 8), the results show that most frameworks lack consideration of vendor lock-in issues. However, as many obtained studies of our analysis are based on ZT providers, it is understandable that they are less likely to address this challenge in their migration methods. Furthermore, the challenge of user disruption during migration is overlooked in most frameworks. This issue is crucial that enterprises planning to migrate to ZTA must consider having a remediation service to support users when there is a service interruption that may impact user productivity.

In addition, the challenge of political resistance is one of the issues that most studies disregard. However, this challenge is essential in the managerial side of migration. Therefore, it is recommended to incorporate a change management plan and strategy to handle political resistance in an enterprise. To harness political resistance, an enterprise should try to get a consensus on the core problem and ensure that negative impacts have been managed appropriately [40].

4) THE EVALUATION RESULTS OF THE PROPOSED FRAMEWORK

From the evaluation results, the proposed ZTA migration framework can provide complete and comprehensive migration details. Overall, the proposed framework is more consistent as it depicts the main processes and sub-processes of migrating to ZTA. In addition, it is optimized by incorporating DevOps methodology, which concerns the whole life cycle of migration in both technical and managerial aspects of ZTA migration.

According to the ZTA-related criteria of framework evaluation, the proposed framework can address all requirements, such as process clarity, traceability, and tailorability. For instance, as for traceability and process clarity criteria, the proposed framework can address these issues as it shows consistent main processes, subprocesses, and the output of each process. In addition, the procedures and supportive

TABLE 10. Studies obtained for final review.

Study	Author	Year	Title	Published in	Publication Type	Classification into Process	Framework Code
[S1]	I. Ahmed, T. Nahar, S.S. Urmi, and K. A. Taher	2020	Protection of Sensitive Data in Zero Trust Model	ICCA 2020: International Conference on Computing Advancements	Conference Paper	II – Context Assessment V – Monitoring and Maintenance	[A1]
[S2]	T. M. S. do Amaral and J. J. C. Gondim	2021	Integrating Zero Trust in the cyber supply chain security	2021 Workshop on Communication Networks and Power Systems (WCNPS)	Conference Paper	II – Context Assessment III – Architect ZTA	[A2]
[S3]	E. Bertino and K. Brancik	2021	Services for Zero Trust Architectures - A Research Roadmap	2021 IEEE International Conference on Web Services (ICWS)	Conference Paper	II – Context Assessment	[A3]
[S4]	D. Tyler and T. Viana	2021	Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture	MDPI	Journal Paper	IV – Zero Trust Transformations	[A4]
[S5]	S. Teerakanok, T. Uehara, and A. Inomata	2021	Migrating to Zero Trust Architecture: Reviews and Challenges	Hindawi: Security and Communication Networks	Journal Paper	II – Context Assessment	[A5]
[S6]	D. Klein	2019	Micro-segmentation: securing complex cloud environments	ELSEVIER: Network Security Volume 2019, Issue 3	Journal Paper	III – Architect ZTA	[A6]
[S7]	Y. Bobbert and J. Scheerder	2021	On the Design and Engineering of a Zero Trust Security Artefact	FICC 2021: Advances in Information and Communication	Conference Paper	I – Strategize Zero Trust	[A7]
[S8]	J. Garbis and J. W. Chapman	2021	Zero Trust Security: An Enterprise Guide	Apress; 1st ed. edition	Book	I – Strategize Zero Trust II – Context Assessment IV – Zero Trust Transformations	[A8]
[S9]	M. J. Haber	2021	Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations	Apress; 2nd ed. edition	Book	II – Context Assessment III – Architect ZTA V – Monitoring and Maintenance VI – Optimize ZTA Security	[A9]

techniques are also provided. The proposed framework offers a low-risk migration strategy to migrate to ZTA in which risk assessment and ZTA mutuality assessment are considered. Moreover, the proposed framework can address the challenges of ZTA migration, as shown in Table 8. For example, for vendor lock-in challenge, the consideration of this issue is discussed in process III – Architect ZTA. Furthermore, the proposed framework aims to solve the problems of analysis paralysis, political resistance, and the discovery of resources. These challenges are clearly elaborated in the process I – Strategize Zero Trust and process II – Context Assessment.

VII. LIMITATIONS

This study has some limitations, namely publication bias and validating of framework, as described below.

1) PUBLICATION BIAS

The studies we found are based on our defined keywords and inclusion and exclusion criteria. However, we only select the studies published in English, which may lead to publication bias. In addition, many studies are ZT vendors' publications to propose their ZTA solutions. Therefore, although many studies provide comprehensive details of their migration practices, they are not fairly neutral as they also offer their ZT solutions for migration.

2) FRAMEWORK VALIDATION

At this stage, we do not have an experimental phase for implementing the proposed ZTA migration framework to validate it. In this research, the validation of the proposed ZTA migration framework is evaluated based on the framework evaluation criteria we developed to assess our

TABLE 10. *(Continued.)* **Studies obtained for final review.**

Study	Author	Year	Title	Publisher	Classification into Process	Framework Code
[S10]	S. Rose, O. Borchert, S. Mitchell and S. Connelly	2021	NIST Special Publication 800-207: Zero Trust Architecture	National Institute of Standards and Technology	I – Strategize Zero Trust II – Context Assessment III – Architect ZTA IV – Zero Trust Transformations	[A10]
[S11]	R. Ward and B. Beyer.	2014	BeyondCorp: A New Approach to Enterprise Security	Google Research	III – Architect ZTA IV – Zero Trust Transformations	[A11]
[S12]	L. Cittadini, B. Spear, B. Beyer, and M. Saltonstall	2016	BeyondCorp: The Access Proxy	Google Research	I – Strategize Zero Trust	[A11]
[S13]	B. Osborn, J. McWilliams, B. Beyer and M. Saltonstall	2016	BeyondCorp: design to deployment at Google	Google Research	IV – Zero Trust Transformations	[A11]
[S14]	H. King, M. Janosko, B. Beyer, and M. Saltonstall	2018	BeyondCorp: Building a Healthy Fleet	Google Research	IV – Zero Trust Transformations	[A11]
[S15]	J. Peck, B. Beyer, C. Beske, and M. Saltonstall	2017	Migrating to BeyondCorp: maintaining productivity while improving security	Google Research	I – Strategize Zero Trust IV – Zero Trust Transformations	[A11]
[S16]	V.M. Escobedo, F. Zyzniewski and M. Saltonstall	2017	BeyondCorp: the user experience	Google Research	IV – Zero Trust Transformations	[A11]
[S17]	Microsoft	2021	Implementing a Zero Trust security model at Microsoft	Microsoft	II – Context Assessment III – Architect ZTA	[A12]
[S18]	Microsoft	2020	Zero Trust Business Plan – Microsoft	Microsoft	I – Strategize Zero Trust V – Monitoring and Maintenance	[A12]
[S19]	ILLUMIO	2019	Achieving Zero Trust With ILLUMIO	Illumio	I – Strategize Zero Trust III – Architect ZTA V – Monitoring and Maintenance	[A13]
[S20]	Palo Alto Networks	2020	Best Practices Implementing Zero Trust with Palo Alto Networks	Palo Alto Networks	I – Strategize Zero Trust II – Context Assessment III – Architect ZTA IV – Zero Trust Transformations V – Monitoring and Maintenance VI – Optimize ZTA Security	[A14]
[S21]	Pricewaterhouse Coopers	2021	Zero Trust architecture: a paradigm shift in cybersecurity and privacy	PricewaterhouseCoopers Consulting Pte. Ltd.	II – Context Assessment III – Architect ZTA V – Monitoring and Maintenance VI – Optimize ZTA Security	[A15]
[S22]	S. Turner *et al*,.	2021	A Practical Guide To A Zero Trust Implementation	Forrester Research	I – Strategize Zero Trust II – Context Assessment III – Architect ZTA	[A16]
[S23]	J. Budge and C. Cunningham	2020	How To Implement Zero Trust Security In Asia Pacific	Forrester Research	I – Strategize Zero Trust	[A16]
[S24]	CISCO	2021	From MFA to Zero Trust: A Five-Phase Journey to Securing the Federal Workforce	Duo Security, Inc.	III – Architect ZTA	[A17]

TABLE 10. *(Continued.)* **Studies obtained for final review.**

[S25]	C. Gero	2021	A Blueprint for Zero Trust Architecture: Actionable Implementation Guide	Akamai Technologies	II – Context Assessment IV – Zero Trust Transformations VI – Optimize ZTA Security	[A18]
[S26]	K.D. Uttecht	2020	Zero Trust (ZT) Concepts for Federal Government Architectures	MIT Lincoln Laboratory	I – Strategize Zero Trust III – Architect ZTA IV – Zero Trust Transformations	[A19]
[S27]	HITACHI	2021	Zero Trust and Access Management: A Journey, Not a Destination	Hitachi ID Systems, Inc.	I – Strategize Zero Trust III – Architect ZTA	[A20]
[S28]	ON2IT	2020	A hands-on approach to Zero Trust implementation	ON2IT	III – Architect ZTA V – Monitoring and Maintenance	[A21]

proposed framework. Besides, the evaluation criteria are also used to evaluate selected published studies from a systematic review.

However, these criteria may not reflect all aspects of ZTA migration, such as the effectiveness of functional components or the efficacy of ZTA after post-migration.

VIII. POTENTIAL FUTURE WORKS

This section suggests potential future works, as described below.

1) EXPERIMENTAL PHASE FOR FRAMEWORK VALIDATION

The present comprehensive ZTA migration framework can be validated to make it more practical and effective by implementing processes and sub-processes in a controlled environment within an enterprise. In addition, a survey regarding implementing the proposed framework can be conducted further to gain insightful opinions and collect information from experts, IT staff, and users. The costs of implementing ZTA should also be surveyed to assess the costs and benefits before making a decision to migrate to the ZT environment.

2) TECHNICAL TECHNIQUES FOR DEPLOYING SECURITY COMPONENTS IN ZTA

ZTA is an integrated security solution that provides dynamic and contextual security controls. It is the coordination and interoperability of essential security domains, including identity, device, network, data, workloads, visibility and analytics, and automation and orchestration. As for potential future work, technical techniques for implementing security components can be researched further to better understand how to deploy security solutions in the ZT environment, such as methods for implementing micro-segmentation, authentication solutions, and access control systems.

3) DEPLOYING ZTA WITH THE CLOUD ENVIRONMENT

Enterprise architectures are becoming more hybrid, with infrastructure that combines cloud and on-premises services. Their data, systems, or applications are hosted on cloud infrastructure and services. However, the expansion of cloud services poses challenges to security and privacy, such as identity theft and data breaches. Therefore, the potential future work can focus on the methods to deploy to ZTA to work well with the cloud environment, for instance, the execution of identity-centric and dynamic access controls for granting access to resources residing in the cloud environment.

IX. CONCLUSION

In this paper, we develop a comprehensive framework for migrating to ZTA. This framework considers an effective and practical process-driven framework for migration. This proposed framework is constructed based on a systematic review by synthesizing and analyzing selected published studies relevant to ZT migration methods and techniques. We present six main processes which combine subprocess and essential components for ZTA migration. The proposed ZTA migration processes are 1) Strategize Zero Trust, 2) context assessment, 3) Architect ZTA, 4) Zero Trust transformation, 5) Monitoring and Maintenance, and 6) optimize ZTA security, respectively. In addition, this proposed migration framework also incorporates DevOps methodology that optimizes the migration framework to be more effective.

We validate the proposed framework by utilizing the framework evaluation criteria to assess the effectiveness and usability of the proposed framework. The evaluation concerns crucial criteria related to software engineering and ZTA-related criteria. In addition, the evaluation criteria are also used to evaluate other ZTA migration frameworks to understand the effectiveness of ZTA migration techniques that other studies propose. The evaluation results show that our

TABLE 11. Main concepts of obtained studies.

Study	Author	Main Concept
[S1]	I. Ahmed, T. Nahar, S.S. Urmi, and K. A. Taher (2020)	The study describes the basic steps of Zero Trust implementation. The steps include identifying and mapping sensitive data flows, architecting the parameters of Zero Trust, and monitoring the Zero Trust ecosystem. The final step is to adopt security automation and orchestration.
[S2]	T. M. S. do Amaral and J. J. C. Gondim	The study aims to provide security controls based on ZTA's principles. The security controls apply to five domains: device, identity, application, governance and data, infrastructures, and networks.
[S3]	E. Bertino and K. Brancik (2021)	The study demonstrates concepts of a ZT model implementation. An enterprise must know about threats and select appropriate ZTA service providers. After implementation, the implementation solutions should be measured against performance metrics.
[S4]	D. Tyler and T. Viana (2021)	This study provides technical concepts on implementing ZTA starting from the stage of implementing basic security, logging, and monitoring the network. The next stage is to implement micro-segmentation and apply further access control.
[S5]	S. Teerakanok, T. Uehara, and A. Inomata (2021)	This study explains three main steps of migration staring from an assessment stage where the actors and assets of an enterprise are identified. The next step is undertaking risk assessment and prioritization to identify low-risk candidates for the first transition. The final step is deploying and reviewing the migration process.
[S6]	D. Klein (2019)	The study describes essential phases of implementing micro-segmentation, starting from the discovery and identification of all applications, and then mapping dependencies. The next phase is grouping applications for rules and creating policies. The next stage is to deploy, monitor, and enforce those policies.
[S7]	Y. Bobbert and J. Scheerder (2021)	This study focuses on creating three levels of plans for ZTA migration. First, an enterprise must establish a strategic plan to understand the environment and capabilities. Second, a managerial plan should be created to know potential risks. Finally, an operational plan should also be created to determine ZT technologies.
[S8]	J. Garbis and J. W. Chapman (2021)	The deployment begins by defining problems, researching ZT solutions, and proposing potential implementation approaches. After that, the migration team performs proof of concept of potential ZT platforms in a non-production environment. Once a pilot instance is successfully deployed, the team can deploy a pilot program in production and validate the results.
[S9]	M. J. Haber (2021)	There are key migration steps, starting from defining sensitive data and mapping the processes of those sensitive data. Then, an enterprise creates the micro-perimeter and monitors the Zero Trust environment. Finally, an enterprise adopts automation and adaptive response.
[S10]	S. Rose, O. Borchert, S. Mitchell and S. Connelly (2021)	This study provides an incremental change approach to the ZTA migration. An enterprise must survey assets and examine and map the business process. Then an enterprise chooses the candidate workflow for initial deployment. The next phase is to extend the ZT deployment.
[S11]	R. Ward and B. Beyer (2014)	The study explains the strategy of implementing ZTA. The significant implementation concerns include identifying the device and user and removing trust from the network. Moreover, an enterprise externalizes applications and workflows and deploys inventory-based access control.
[S12]	L. Cittadini, B. Spear, B. Beyer, and M. Saltonstall (2016)	This study provides methods to handle exceptional cases and exceptions for transitioning to ZTA. In addition, the study emphasizes the importance of coordination and integration of multiple teams for migration.
[S13]	B. Osborn, J. McWilliams, B. Beyer and M. Saltonstall (2016)	The study explains the methods to deploy the initial rollout of the candidate workflows. The focus is to deploy ZTA without user disruptions and provide a method for users to be self-remediate.
[S14]	H. King, M. Janosko, B. Beyer, and M. Saltonstall (2018)	The study describes an approach to handle exceptions for the ZT project. An enterprise should determine procedures and technical implementation for exception management.
[S15]	J. Peck, B. Beyer, C. Beske, and M. Saltonstall (2017)	The study shows how to roll out the ZT migration in phases. The pilot program begins to roll out in a small-scale pilot. The rollout increases over time and expands to the risky workflows after learning from a history of success and gaining more confidence in the strategy.
[S16]	V.M. Escobedo, F. Zyzniewski and M. Saltonstall (2017)	The study emphasizes the importance of communicating with users regarding ZTA early. Moreover, new devices will be set up and automatically configured to access the ZT environment. In addition, the study explains the methods to reduce VPN usage.
[S17]	Microsoft (2021)	Four primary services need to be verified for implementation. An enterprise must verify the identity of users and register devices into the device management system. In addition, the access must be verified to segment users and devices. Finally, the services must be verified to enable conditional access.
[S18]	Microsoft (2020)	The study describes two main stages of migrating to ZTA. First, the planning stage involves defining a vision, getting buy-in from stakeholders, and defining the scope of implementation. In the measurement stage, an enterprise should measure security effectiveness after successfully implementing ZTA.
[S19]	ILLUMIO (2019)	The essential steps to migrate to ZTA are as follows. 1) an enterprise defines a vision with key stakeholders. 2.) Identifying and mapping data flows. 3) implementing micro-segmentation. 4) mitigating vulnerabilities and prioritizing risks. 5) automation and orchestration security processes.
[S20]	PaloAlto Networks (2020)	There are five main steps of implementing ZTA. 1) an enterprise defines the protected surface. 2) The protected surface is mapped to transaction flows. 3) an enterprise architects a ZT network 4) The ZT policies are created. Finally, 5) an enterprise monitor and maintain the ZT network.
[S21]	Pricewaterhouse Coopers (2021)	The study describes five main steps of migrating to ZTA. 1) identifying sensitive data 2) Defining sensitive data flows 3) Defining micro-perimeter network 4) Creating security policies and control framework. 5) Continuously monitoring the ZT network.
[S22]	S. Turner, *et al.* (2021)	The study shows a practical guide to implementing ZTA. The first step is to perform program mobilization to establish the ZT project plans. The next step is implementing the ZT solutions to protect users, devices, workloads, and networks.

TABLE 11. *(Continued.)* **Main concepts of obtained studies.**

[S23]	J. Budge and C. Cunningham (2020)	The study focuses on defining key stakeholders in implementing ZTA. The key stakeholders concern many teams in an enterprise, such as the management, audit and compliance team, operational team, and security team.
[S24]	CISCO (2021)	The study shows five phases of implementing ZTA. Phase 1 is to establish user trust and Phase 2 is to implement device and activity visibility. At phase 3, it is to establish device trust. Phase 4 creates adaptive policies, and phase 5 utilizes Zero Trust for the federal workforce.
[S25]	C. Gero (2021)	The study describes three main stages of the ZTA migration, starting from the planning stage for the ZT. The second stage is to perform user grouping for the migration. The next stage is to deploy the application rollout for ZTA.
[S26]	K.D. Uttecht (2020)	The study describes essential methods for migrating to ZTA. Firstly, an enterprise must have a clear plan for the ZT project and get stakeholder buy-in. Then, the enterprise gathers information about assets and creates use cases of how ZT will be implemented.
[S27]	HITACHI (2021)	The study describes critical steps to migrate to ZTA, starting from gaining leadership and stakeholders' support. The next step is to select the ZT migration team and assess the current environment. The next phase is to review the available ZT technologies, plan the ZT activities, and identify operational changes.
[S28]	ON2IT (2020)	The study explains five main steps to migrating to ZTA. 1) Define and classify the protected surface 2) Map the transaction flows 3) Architect a ZT network 4) Establish the ZT policies 5) Monitor and maintain the ZT network.

TABLE 12. **Framework evaluation – generic criteria.**

No.	Evaluation criterion	Evaluation question	Criterion Type	Description
1.	Process Clarity	Does the framework provide a clear description of the suggested processes and activities?	Scale	■ The framework explicitly provides a clear description of the activities for conducting ZTA migration process. ◧ The framework provides a general description for some processes, but details are lacking. ☐ The framework provides either very partial description or no description for the processes or activities.
2.	Procedures & Supportive Techniques	Does the framework provide procedures or supportive techniques to perform each process?	Scale	■ The framework offers techniques or examples for each ZTA migration process. ◧ The framework offers techniques or examples for some activities in the ZTA migration process. ☐ The framework does not provide supportive techniques or examples for the ZTA migration process.
3.	Traceability	Does the framework identify the sequence of modelling or dependencies between processes?	Scale	■ The framework specifies traceability or dependencies in the migration process. ◧ The framework specific traceability for a subset of activities in the migration process. ☐ Traceability or dependencies links between processes have not been specified.
4.	Tailorability	Is the framework based on a one-fits-all assumption or define adaptative mechanisms for migration? Is the framework be expressed in the form of method fragments or process components?	Scale	■ The framework explicitly defines mechanisms to configure and modify its suggested process. ◧ The framework provides a basis of method fragments or process components so that the tailoring process can be facilitated. ☐ There is no method fragments or process components that supports tailoring by the framework.
5.	Tool Support	Does the framework suggest or provide guidelines of the tools that support the ZTA migration process?	Scale	■ The framework clearly suggests or provides tools for the whole ZTA migration process. ◧ The framework suggests or provides tools for some activities in the ZTA migration process. ☐ The framework neither provides tools nor refers to tools for the ZTA migration.
6.	Scalability	Is the framework applicable to handle various migration sizes?	Boolean	Yes: The framework explicitly defines mechanisms to support various migration sizes and its scalability has been demonstrated in a real project. No: The framework does not support scalability.
7.	Formality	Does the framework provide a degree of formality on technical aspects?	Boolean	Yes: The framework provides formal techniques for some activities. No: There is no formalism supported by the framework.
8.	Theoretical foundation	Is the framework inspired or developed based on the existing software engineering paradigms or practice?	Descriptive	
9.	Work-Products	What work-products are described by the framework to produce in the ZTA migration process?	Descriptive	
10.	Development Roles	What development roles, who are responsible for performing migration activities or any stakeholder who are involved, are defined by the framework?	Descriptive	
11.	Domain Applicability	What are application domains for which the framework offer?	Descriptive	

proposed ZTA migration framework can comprehensively cover all the criteria of framework evaluation and provide complete and consistent processes for migrating to ZTA. Thus, the proposed comprehensive ZTA migration framework can be used as a reference model for effective transitioning to Zero Trust Architecture.

TABLE 13. Framework evaluation – zero trust migration challenges criteria.

No.	Evaluation criterion	Evaluation question	Criterion Type	Description
1.	Vendor Lock-in	Does the framework provide a clear description or mechanisms to manage Zero Trust vendor lock-in issues?	Scale	■ The framework offers clear techniques or examples for to manage Zero Trust vendor lock-in issues in the migration process. ◧ The framework offers techniques or examples for some activities to manage Zero Trust vendor lock-in issues. ☐ The framework does not provide supportive techniques or example for activities to manage Zero Trust vendor lock-in issues.
2.	Analysis Paralysis	What are the strategies or techniques to analyze or perform activities of the migration process?	Scale	■ The framework explicitly offers strategies or techniques to analyze or perform activities of the migration process. ◧ The framework offers general strategies or techniques to analyze or perform some activities of the migration process. ☐ The framework does not provide supportive strategies or techniques to analyze or perform activities of the migration process.
3.	Integration Issues	Does the framework provide a clear description or mechanisms to manage integration issues?	Scale	■ The framework explicitly offers clear techniques or examples for to manage integration issues in the migration process. ◧ The framework offers techniques or example for some activities to manage integration issues. ☐ The framework does not provide supportive techniques or example for activities to manage integration issues.
4.	Legacy systems	Does the framework provide a clear description or mechanisms to manage legacy systems issues?	Scale	■ The framework explicitly offers clear techniques or examples for to manage legacy systems issues in the migration process. ◧ The framework offers techniques or example for some activities to manage legacy systems issues. ☐ The framework does not provide supportive techniques or example for activities to manage legacy systems issues.
5.	Discovery Resources	Does the framework define techniques or mechanisms to discover resources?	Scale	■ The framework explicitly defines techniques or mechanisms to discover resources. ◧ The framework provides a basis of method fragments so that discovery resources can be facilitated. ☐ There is no discover resources techniques or mechanisms supported by the framework.
6.	User Disruptions During Migration	Does the framework provide a clear description or mechanisms to manage user disruptions during migration?	Scale	■ The framework explicitly offers clear techniques or examples for to manage user disruptions in the migration process. ◧ The framework offers techniques or example for some activities to manage user disruptions in the migration process. ☐ The framework does not provide supportive techniques or example for activities to manage user disruptions in the migration process.
7.	ZTA Service Controls	Does the framework provide clear techniques or tools to support ZTA service controls or a ZT platform?	Scale	■ The framework explicitly provides clear techniques or tools to support ZTA service controls or a ZT platform. ◧ The framework provides techniques or tools for some activities to support ZTA service controls or a ZT platform. ☐ The framework neither provides techniques or tools to support ZTA service controls or a ZT platform.
8.	Application of Industry Standard	Does the framework apply industry standard regarding Zero Trust migration or implementation in their migration process?	Scale	■ The framework explicitly specifies applying industry standards for conducting the migration process. ◧ The framework specifies applying industry standards for conducting the migration process for some activities. ☐ The framework does not specify applying industry standards for conducting the migration process.
9.	Regulatory Compliance	Does the framework take regulatory compliance into consideration in the migration process?	Scale	■ The framework explicitly specifies consideration of regulatory compliance for conducting the migration process. ◧ The framework specifies consideration of regulatory compliance for conducting the migration process for some activities. ☐ The framework does not specify consideration of regulatory compliance for conducting the migration process.
10.	Political Resistance	Does the framework provide methods or techniques to manage political resistance in the migration?	Scale	■ The framework explicitly specifies methods or techniques to manage political resistance in the migration. ◧ The framework specifies methods or techniques to manage political resistance for some activities in the migration. ☐ The framework does not specify methods or techniques to manage political resistance in the migration.

TABLE 13. *(Continued.)* **Framework evaluation – zero trust migration challenges criteria.**

11.	Zero Trust Policies	Does the framework provide methods or techniques to establish and manage Zero Trust Policy?	Scale	■ The framework explicitly provides methods or techniques to establish and manage Zero Trust Policy. ◧ The framework provides methods or techniques to establish and manage Zero Trust Policy but details are lacking. ☐ The framework does not provide methods or techniques to establish and manage Zero Trust Policy.

APPENDIX A
QUALITY ASSESSMENT CHECKLIST OF GREY LITERATURE FOR SOFTWARE ENGINEERING [22]

See Table 9.

APPENDIX B
A. IDENTIFICATION OF STUDIES VIA ACADEMIC DATABASE

See Table 10.

B. IDENTIFICATION OF STUDIES VIA OTHER METHODS

See Table 11.

APPENDIX C

This appendix shows framework evaluation criteria and evaluation results of the study. See Tables 12 and 13.

REFERENCES

[1] American Council for Technology-Industry Advisory Council (ACT-IAC). (2019). *Zero Trust Cybersecurity Current Trends*. Accessed: Nov. 25, 2022. [Online]. Available: https://www.actiac.org/documents/zero-trust-cybersecurity-current-trends

[2] M. Bowen. *Survey Reveals Zero Trust Adoption Appealing But Challenging*. Accessed: Nov. 26, 2022. [Online]. Available: https://www.intelligentcio.com/north-america/2021/09/16/survey-reveals-zero-trust-adoption-appealing-but-challenging/

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly. *NIST Special Publication 800–207 Zero Trust Architecture*. National Institute of Standards and Technology. US Department of Commerce. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[4] CISCO. (2021). *From MFA to Zero Trust: A Five-Phase Journey to Securing the Federal Workforce*. CISCO SECURE. Accessed: Nov. 25, 2022. [Online]. Available: https://www.meritalk.com/wp-content/uploads/2021/06/mfa-to-zero-trust.pdf

[5] R. Ward and B. Beyer, "BeyondCorp: A new approach to enterprise security," *Login*, vol. 39, no. 6, pp. 6–11, Dec. 2014. [Online]. Available: https://www.usenix.org/system/files/login/articles/login_dec14_02ward.pdf

[6] B. Osborn, J. McWilliams, B. Beyer, and M. Saltonstall, "BeyondCorp: Design to deployment at Google," *Login*, vol. 41, no. 1, pp. 28–34, 2016. [Online]. Available: https://www.usenix.org/system/files/login/articles/login_spring16_06_osborn.pdf

[7] Microsoft. *Implementing a Zero Trust Security Model at Microsoft*. Accessed: Nov. 27, 2022. [Online]. Available: https://www.microsoft.com/en-us/insidetrack/implementing-a-zero-trust-security-model-at-microsoft

[8] Microsoft. *Zero Trust Business Plan—Microsoft*. Accessed: Nov. 27, 2022. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJtxq

[9] I. Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, "Protection of sensitive data in zero trust model," in *Proc. Int. Conf. Comput. Advancements*, Jan. 2020, pp. 1–5, doi: 10.1145/3377049.3377114.

[10] M. J. Haber, *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*, 2nd ed. New York, NY, USA: Apress, 2020.

[11] R. Mass. *A Hands-on Approach to Zero Trust Implementation*, ON2IT, Gelderland, The Netherlands, 2020. [Online]. Available: https://www.cymbel.com/wp-content/uploads/2020/10/A-hands-on-approach-to-Zero-Trust-implementation.pdf

[12] Palo Alto Networks, Inc. (2022). *Best Practices Implementing Zero Trust With Palo Alto Networks*. [Online]. Available: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/best-practices/zero-trust-best-practices/zero-trust-best-practices.pdf

[13] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to zero trust architecture: Reviews and challenges," *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, May 2021, doi: 10.1155/2021/9947347.

[14] B. Ali, S. Hijjawi, L. H. Campbell, M. A. Gregory, and S. Li, "A maturity framework for zero-trust security in multiaccess edge computing," *Secur. Commun. Netw.*, vol. 2022, pp. 1–14, Jun. 2022, doi: 10.1155/2022/3178760.

[15] *Zero Trust Maturity Model (Pre-Decisional Draft)*, Cybersecurity and Infrastructure Security Agency (CISA), Arlington, VA, USA, 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[16] K. D. Uttecht, "Zero trust (ZT) concepts for federal government architectures," Lincoln Lab., Massachusetts Inst. Technol., Lexington, MA, USA, Tech. Rep. TR-1253, 2020. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1108910.pdf

[17] K. E. Foltz and W. R. Simpson, "Zero trust technology integration issues," Inst. Defense Analyses, Alexandria, VI, USA, Tech. Rep. IDA NS D-22663, 2021. [Online]. Available: https://www.jstor.org/stable/resrep34846

[18] E. Bertino and K. Brancik, "Services for zero trust architectures—A research roadmap," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Sep. 2021, pp. 14–20, doi: 10.1109/ICWS53863.2021.00016.

[19] E. B. Fernandez and A. Brazhuk, "A critical analysis of zero trust architecture (Zta)," *SSRN Electron. J.*, vol. 2022, pp. 1–16, Sep. 2022, doi: 10.2139/ssrn.4210104.

[20] J. Garbis and J. W. Chapman, *Zero Trust Security: An Enterprise Guide*, 1st ed. New York, NY, USA: Apress, 2021.

[21] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Syst. Rev.*, vol. 10, no. 89, Mar. 2021, Art. no. 105906, doi: 10.1186/s13643-021-01626-4.

[22] V. Garousi, M. Felderer, and M. V. Mäntylä, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Inf. Softw. Technol.*, vol. 106, pp. 101–121, Feb. 2019.

[23] J. Münch, "Data- and value-driven software engineering with deep customer insight: Proceedings of the seminar no. 58314308," Univ. Helsinki, Dept. Comput. Sci., Tech. Rep., 2014. [Online]. Available: http://hdl.handle.net/10138/152785

[24] S. Badshah, A. A. Khan, and B. Khan, "Towards process improvement in DevOps: A systematic literature review," in *Proc. Eval. Assessment Softw. Eng.*, 2020, pp. 427–433, doi: 10.1145/3383219.3383280.

[25] P. Jha and R. Khan, "A review paper on DevOps: Beginning and more to know," *Int. J. Comput. Appl.*, vol. 180, no. 48, pp. 16–20, Jun. 2018, doi: 10.5120/ijca2018917253.

[26] S. Turner, D. Holmes, C. Cunningham, J. Budge, P. McKay, A. Cser, H. Shey, and M. Maxim, "A practical guide to a zero trust implementation," Forrester Research, Inc., Cambridge, MA, USA, Tech. Rep. 157736, Mar. 2021.

[27] *Zero Trust and Access Management: A Journey, Not a Destination*, Hitachi ID Systems, Inc., Calgary, AB, Canada, 2021.

[28] *Achieving Zero Trust With ILLUMIO*, Illumio, Inc., Sunnyvale, CA, USA, 2020. [Online]. Available: https://www.illumio.com/sites/default/files/2021-02/achieving-zero-trust-20sb10%20%281%29.pdf

[29] Y. Bobbert and J. Scheerder, "On the design and engineering of a zero trust security artefact," in *Proc. Future Inf. Commun. Conf.*, 2021, pp. 830–848, doi: 10.1007/978-3-030-73100-7_58.

[30] L. Cittadini, B. Spear, B. Beyer, and M. Saltonstall, "BeyondCorp: The access proxy," *Login*, vol. 41, no. 4, pp. 1–6, 2016. [Online]. Available: https://www.usenix.org/system/files/login/articles/login_winter16_05_cittadini.pdf
[31] J. Budge and C. Cunningham, "How to implement zero trust security in Asia Pacific," Forrester Research, Inc., Cambridge, MA, USA, Tech. Rep. 162457, Oct. 2020.
[32] J. Peck, B. Beyer, C. Beske, and M. Saltonstall, "Migrating to BeyondCorp: Maintaining productivity while improving security," *Login*, vol. 42, no. 2, pp. 1–7, 2017. [Online]. Available: https://www.usenix.org/system/files/login/articles/login_summer17_10_peck.pdf
[33] T. M. S. do Amaral and J. J. C. Gondim, "Integrating zero trust in the cyber supply chain security," in *Proc. Workshop Commun. Netw. Power Syst. (WCNPS)*, Nov. 2021, pp. 1–6, doi: 10.1109/WCNPS53648.2021.9626299.
[34] C. Gero, "A blueprint for zero trust architecture: Actionable implementation guide," Akamai Technologies, Inc., Cambridge, MA, USA, Tech. Rep., 2021. [Online]. Available: https://www.intelligentcio.com/me/wp-content/uploads/sites//2022/05/A-Blueprint-for-Zero-Trust-Architecture-WP.pdf
[35] *Zero Trust Architecture: A Paradigm Shift in Cybersecurity and Privacy*, PricewaterhouseCoopers Consulting, Singapore, 2021. [Online]. Available: https://www.pwc.com/sg/en/publications/assets/page/zero-trust-architecture.pdf
[36] D. Klein, "Micro-segmentation: Securing complex cloud environments," *Netw. Secur.*, vol. 2019, no. 3, pp. 6–10, Mar. 2019, doi: 10.1016/s1353-4858(19)30034-0.
[37] V. M. Escobedo, F. Zyzniewski, and M. Saltonstall, "BeyondCorp: The user experience," *Login*, vol. 42, no. 3, pp. 6–11, 2017. [Online]. Available: https://www.usenix.org/system/files/login/articles/login_fall17_08_escobedo.pdf
[38] H. King, M. Janosko, B. Beyer, and M. Saltonstall, "BeyondCorp: Building a healthy fleet," *Login*, vol. 43, no. 3, pp. 1–7, 2018. [Online]. Available: https://www.usenix.org/system/files/login/articles/login_fall18_05_king.pdf
[39] M. F. Gholami, F. Daneshgar, G. Low, and G. Beydoun, "Cloud migration process—A survey, evaluation framework, and open challenges," *J. Syst. Softw.*, vol. 120, pp. 31–69, Oct. 2016, doi: 10.1016/j.jss.2016.06.068.
[40] V. J. Mabin, S. Forgeson, and L. Green, "Harnessing resistance: Using the theory of constraints to assist change management," *J. Eur. Ind. Training*, vol. 25, no. 2/3/4, pp. 168–191, Mar. 2001, doi: 10.1108/eum0000000005446.

PACHAREE PHIAYURA received the B.S. degree in political science from Thammasat University, Thailand, and the M.S. degree in information systems from Melbourne University, Australia. She is currently pursuing the M.S. degree in cybersecurity and information assurance with Mahidol University, Thailand. She is a Standard Analyst with the Electronic Transactions Development Agency (ETDA) under the Ministry of Digital Economy and Society, Thailand. Her research interests include cybersecurity, information security, enterprise architectures, and emerging technologies and issues.

SONGPON TEERAKANOK received the B.E. degree from the Prince of Songkla University, Thailand, in 2013, and the M.E. and D.Eng. degrees in information science and engineering from Ritsumeikan University, in 2016 and 2019, respectively. He was a former Assistant Professor at Ritsumeikan University. He joined the Faculty of ICT, Mahidol University, Thailand, in May 2021. His research interests include cryptography, cybersecurity, privacy, location-based service (LBS), and digital forensics.