JHSS (Journal of Humanities and Social Studies) *Volume 10, Number 02, Page 1045-1050*
https://jhss-lppmunpak.id/index.php/jhss *e-ISSN: 2598-120X; p-ISSN: 2598-117X*

EVALUATION OF A ZERO TRUST–BASED CYBERSECURITY STRATEGY: A CASE STUDY OF PT XYZ

Rani Fersari Damanik [a*)], Setiadi Yazid [a)] , Yudho Giri Sucahyo [a)]

[a)] *Universitas Indonesia, Depok, Indonesia*

[*)]*Corresponding Author: rani.fersari@ui.ac.id*

Article history: received 19 May 2026; revised May 26, 2026; accepted 26 June 2026 *DOI: https://doi.org/10.33751/jhss.v10i2.126*

Abstract. Zero Trust (ZT) has become a fundamental paradigm in modern cybersecurity architecture by emphasizing the principle of "never trust, always verify." The Cybersecurity and Infrastructure Security Agency (CISA) introduced the Zero Trust Maturity Model (ZTMM) as a framework to guide organizations through four maturity stages Traditional, Initial, Advanced, and Optimal in adopting Zero Trust principles in a gradual and structured manner. In Indonesia, PT XYZ, as one of the telecommunications companies in the country, has adopted the Zero Trust approach as a strategy to strengthen its overall security posture amid the increasing complexity of infrastructure and cyber threats. This study aims to evaluate the maturity level of Zero Trust implementation at PT XYZ using the CISA ZTMM framework. The evaluation was conducted by analyzing the implementation of security controls across several core pillars of Zero Trust and assessing the alignment of these implementations with the defined maturity levels. The measurement results indicate that the maturity level of Zero Trust implementation at PT XYZ is currently at the Initial level, characterized by the partial implementation of Zero Trust controls and the suboptimal integration across security domains. These findings indicate the existence of gaps in aspects such as visibility, automation, governance, and cross-pillar capabilities that hinder the organization from achieving a higher level of maturity. The results of this study are expected to serve as a basis for developing strategic recommendations and an implementation roadmap for Zero Trust to support advancement toward the Optimal level.

Keywords: Zero Trust, Zero Trust Maturity Model, CISA, Cybersecurity

I. INTRODUCTION

The concept of Zero Trust, was first introduced to address the problems posed by threats from the Company's internal parties [1]. Zero Trust Architecture (ZTA) is a new security approach to building secure systems. ZTA establishes the principle that no entity, either internal or external to an organization's network, can be trusted automatically without going through a verification process [2]. Zero Trust provides data protection, even when employees access it from off-site using personal devices [3]. This is important given the increasing trend of remote work adoption and personal device use by employees, which can increase the risk of data leaks and threats to information security. The implementation of zero trust is a complex process that covers various dimensions in the security system [3].

The Zero Trust security model no longer relies on perimeter-based security, but instead uses short-term connections with strong authentication, dynamic trust, and adaptive risk assessment through complex security strategies [4]. Thus, *Zero Trust* is not only a technical security framework, but also an important strategy to protect an organization's data, infrastructure, and operational continuity in the midst of ever-evolving cyber threats [5].

The main components of ZTA include Identity and Access Management (IAM), continuous authentication, the application of the principle of least privilege, microsegmentation, and real-time monitoring [6]. These principles ensure that access is only granted after going through a thorough validation process, so as to suppress the potential for lateral movements by malicious parties. Recent studies show that the implementation of ZTA in cloud, hybrid, and remote working environments can improve security visibility and strengthen data protection mechanisms [7]. Zero Trust therefore plays a role not only as a technical solution, but also as a long-term security strategy that supports the resilience of information systems as a whole.

PT XYZ, one of the telecommunications companies in Indonesia, faces challenges in maintaining the security of IT infrastructure from increasingly complex cyber threats. As digital technology develops and the reliance on information systems increases, cyberattacks such as malware, hacking, phishing, and data theft are becoming more frequent and more difficult to detect. The conventional security approach that has been based on the perimeter model, which relies on network boundaries to distinguish between trustworthy entities within the network and those that are not trusted outside, is no longer adequate. This model has a fundamental weakness because it gives implicit trust to internal entities, which can actually be used by parties who have successfully infiltrated or by insider threat actors.

In an effort to overcome these challenges, PT XYZ adopts the ZTA approach as the main strategy in strengthening the company's network security and data protection systems. Through the implementation of Zero Trust, PT XYZ seeks to build an IT environment that is more resilient to cyber attacks, reduce the risk of data leaks, and increase visibility and control over all activities on the network. In addition, this approach also allows for the implementation of more adaptive and risk-based security policies in accordance with the evolving threat dynamics. The implementation of ZTA is expected to be able to support the sustainability of the company's operations by maintaining integrity, confidentiality, and overall information availability. The question of this research is "what is the maturity level of Zero Trust implementation in XYZ companies?"

\

II. RESEARCH METHODS

This study analyzed the maturity level of Zero Trust implementation using the Zero Trust Maturity Model (ZTMM) framework developed by CISA. The flexibility and comprehensive scope make this framework relevant for various types of organizations, including in the government and private sectors [8].

This model provides a systematic approach to assessing an organization's progress in adopting Zero Trust principles. ZTTM offers actionable and tailored guidance for various regulatory environments as well as helps evaluate maturity levels, providing a clear path for practical implementation and organizational development [9].

ZTMM consists of five main pillars, each of which is supported by cross-functional capabilities, namely Visibility and Analytics, Automation and Orchestration, and Governance. This capability enables integration both within and between pillars, thereby increasing interoperability and supporting a gradual optimization process [9].

A. Identity

This pillar focuses on identifying, authenticating, and managing user access through the implementation of access control policies to verify users connected to the network, leveraging dynamic and contextual data analysis to ensure access is provided to users at the right time [10]. This can be achieved through the implementation of strong authentication, context-based authorization, and identity risk assessment to prevent excessive granting of access rights [9].

B. Devices

Devices refer to a variety of hardware assets that access data on the Internet, such as smartphones, IoT (Internet of Things) devices, laptops, Bring Your Own Devices (BYODs), partner-managed devices, and hosted cloud servers [3]. This diversity provides a very wide attack surface for cybercriminals to attack. Organizations must ensure the basic boundaries of device security protection as well as the visibility of the device itself [8].

C. Network

A network is an open communication medium that includes a variety of channels, such as an organization's internal network, wireless network, and the internet, as well as other potentially usable channels, such as mobile networks and application-level channels for message transmission [8]. The network dimension of a Zero Trust implementation essentially involves network segmentation, isolation, and control. This is considered a crucial point in a zero trust strategy, as when an attacker manages to gain access to a network, they have the potential to have access to the entire network [3].

D. Application and Workload

Applications and workloads include computer programs, organizational systems, and services that can run in on-premises environments, mobile devices, or cloud environments [9]. This pillar shifts the focus from traditional accreditation boundaries to treating externally facing applications, ensuring secure delivery with granular access controls and integrated threat protection across all *deployment* environments [10].

E. Data

In *a Zero Trust* architecture, data security focuses on data management, data grouping or classification, designing classification schemes, and implementing encryption both when data is being transmitted and when it is stored [3]. Data is often a prime target for attackers, so a Zero Trust framework puts data protection first. Therefore, organizations need to understand where data is stored, how the data is classified, who has access, and monitor and control data access through the use of policies set by the policy engine.

III. RESULT AND DISCUSSION

While CISA ZTMM provides a valuable high-level framework, it does not yet have the level of granularity necessary for organizations to quantitatively assess their current security posture and strategically plan their next steps. Currently, there is no standardized assessment system that can provide an accurate measure of an organization's Zero Trust maturity level [11].

To address these limitations, the study [11], proposed a new quantitative assessment system designed to complement the CISA ZTMM. This system allows organizations to self-evaluate the maturity level of Zero Trust more precisely and develop a focused implementation strategy. This scoring system is directly aligned with the CISA ZTMM framework. Each security function in the five core pillars is assigned a numerical score that reflects its contribution to a particular level of maturity. The maximum score that can be achieved for the Optimal maturity level is 100, while the Advanced, Initial, and Traditional levels have maximum scores of 80, 60, and 40, respectively [11]. In addition, this model also integrates cross-functional capabilities namely Visibility and Analytics, Automation and Orchestration, and Governance. as the main supporting elements in the implementation and evaluation of Zero Trust. This granular assessment approach provides a more measurable framework that allows

Volume 10, Number 02, Page 1045-1050
e-ISSN: 2598-120X; p-ISSN: 2598-117X

organizations to take more appropriate steps in implementing and improving their Zero Trust security posture [11].

In addition, this assessment approach allows organizations to identify gaps (gap analysis) in each pillar and capability more specifically, so that improvement priorities can be determined systematically. Through structured score mapping, organizations not only get an idea of the current level of maturity, but also a clear direction of transformation towards a higher level. This supports data-driven decision-making, especially in designing a sustainable Zero Trust implementation roadmap that aligns with business needs and organizational risk profiles.

The evaluation of the maturity level of Zero Trust implementation at PT XYZ was carried out through filling out a questionnaire prepared based on five main pillars and three cross-functional capabilities, where each question was designed to measure the actual condition of the organization according to the level of maturity. The questionnaire was filled out by three departments responsible for the main pillars, with respondents who were Senior Engineers who had more than five years of work experience at PT XYZ, so that the assessment results obtained were considered representative and credible. Furthermore, the responses that have been collected are processed using a predetermined assessment system to produce a maturity score as a whole and per pillar, which is then presented in the form of a report that includes assessment results and recommendations for improvement.

A. Zero Trust Maturity Evaluation

Based on the results of the Zero Trust Maturity evaluation in Table 1, an assessment was carried out on five main dimensions, namely Identity, Devices, Networks, Applications and Workloads, and Data. The results showed that PT XYZ obtained a Maturity Score of 60 out of a maximum of 100. The Maturity Gap value in each dimension indicates a gap between the current conditions of Zero Trust implementation and the expected ideal conditions. This shows that although a number of security controls have been implemented, there is still a need to improve and strengthen security policies and mechanisms, especially in the Networks, Applications and Workloads, and Data dimensions which have a relatively higher level of gap than other dimensions.

Table 1. Evaluation Results

Pillar	Maturity Score	Maximum Score	Maturity Gap
Identity	14	20	6
Device	13	20	7
Networks	11	20	9
Applications and Workloads	11	20	9
Data	11	20	9

Furthermore, based on the classification of maturity level in Table 2, the total score of 60 is in the range of 41–60 so it is categorized at the Initial level. This level indicates that organizations have begun to adopt the basic concepts and principles of Zero Trust, but the implementation is still in its early stages and has not been thoroughly integrated across all security dimensions.

Table 2. Level Maturity

Total Score	Level
0 - 40	Traditional
41 - 60	Initial
61 - 80	Advanced
81 - 100	Optimal

At the Initial level, the implementation of Zero Trust is still limited to basic security controls and is not supported by comprehensive automation and policy integration. This condition shows that implementation is still partial and has not been able to provide consistent protection at all levels of infrastructure.

B. Analysis of the Maturity Level of Each Pillar

In the Identity pillar, PT XYZ obtained a score of 14 out of 20 in Table 3, which shows that the organization has had quite good capabilities in the implementation of basic identity control. The implementation of the authentication mechanism has included the use of multi-factor authentication (MFA) as well as structured management of user identities, thus placing the organization at the Initial stage within the CISA ZTMM framework. However, when compared to the characteristics of the Optimal level, there are still significant gaps, especially in the aspects of continuous identity validation and risk-based access control. The identity verification process is currently still in the early stages of access and has not taken place continuously verification, while identity risk assessments are still static and have not been supported by real-time-based analytics. In addition, integration between identity stores is not yet fully integrated, limiting the visibility and consistency of identity management across the system environment. The application of the least privilege principle is also not optimal because it has not been supported by the just-in-time (JIT) and just-enough access (JEA) mechanisms. To achieve a higher level of maturity, PT XYZ is increasing the use of phishing-resistant MFA, integrating all identity sources, as well as adopting a risk-based approach supported by real-time analytics. This effort is in line with the core principles of Zero Trust which emphasize that identity verification should be done in an adaptive and continuous manner, not only at the beginning of the authentication process, but throughout the access to resources lifecycle [8].

In the Devices pillar, PT XYZ obtained a score of 13/20 shown in Table 4, this shows the position at the Initial level within the CISA ZTMM framework. Organizations already have basic capabilities such as asset inventory, visibility into most devices, and device management policies. However, there are still gaps in the aspects of continuous compliance monitoring that are not yet real-time and device threat protection that is still partial and not yet integrated (e.g. centralized EDR). To reach a higher level, PT XYZ needs to improve continuous and real-time monitoring of devices, integrate end-to-end threat protection, and implement automation in device management, including isolation and automated remediation. This is important to support the Zero Trust principle which emphasizes continuous verification of devices [8].

The value in the Networks pillar of 11/20 in Table 5 shows a significant maturity gap, with the position of PT XYZ still

Volume 10, Number 02, Page 1045-1050
e-ISSN: 2598-120X; p-ISSN: 2598-117X

dominated by the Traditional level and some are starting to move towards Initial. Network architecture still relies on macro segmentation and perimeter-based security approaches, so it does not support micro-segmentation and dynamic network policies. Although there has been a basic implementation of encryption and traffic management, both are still static and not yet adaptive to risk. In terms of visibility and analytics, monitoring is still limited to compromise indicators without real-time cross-system telemetry correlation. In addition, the aspects of automation, resilience, and governance are also still low and tend to be manual and reactive. Overall, the main weakness lies in the lack of granularity of control, automation, and the lack of implementation of the principle of least privilege connectivity. To achieve the optimal level, a transformation towards micro-segmentation, risk-based dynamic policies, and a more distributed network architecture according to Zero Trust principles [8] is needed.

In the Applications and Workloads pillar with a score of 11/20 in Table 6, PT XYZ is still at the Traditional level with a small increase towards Initial. Organizations have implemented basic practices such as separation of development and production environments and simple access controls, but security integration across the entire application lifecycle (DevSecOps) has not been optimal. The application security testing process is still partial and not yet automated, while application threat protection is still generic and has not been integrated into the application workflow. In addition, the application access mechanism is still based on static authorization and has not implemented context-based continuous authorization. The aspects of visibility, automation, and governance are also still limited and tend to be manual. To achieve the optimal level, it is necessary to integrate end-to-end security in the application lifecycle, implement continuous authorization, and strengthen Zero Trust-based access control with an assume breach approach [8].

The value of the Data pillar with a score of 11/20 in Table 7, PT XYZ is still at the Traditional level with several initial initiatives towards Initial. Organizations have implemented basic access controls as well as some encryption mechanisms to protect data, but overall data management is still unintegrated and adaptive. The main weakness can be seen in the data classification and labeling process which is still carried out manually, so that it is not able to keep up with changes in data sensitivity dynamically. In addition, access control to data is still static and has not implemented context-based or risk-based dynamic data access controls. Visibility, automation, and governance aspects are also still limited, with data monitoring and management not yet supported by adequate analytics and automation. To achieve the Optimal level, PT XYZ needs to implement automatic data classification and labeling, implement dynamic access control, and expand data encryption both at rest, in transit, and in use. In addition, the application of data loss prevention based on behavioral analytics is important to ensure data protection throughout its lifecycle, in line with the Zero Trust principle that places data as the center of protection [8].

Table 3. Maturity Score Pilar Identity

Category	Identity (14/20)				Cross-Cutting capabilities		
Function	**Authentication**	**Identity Stores**	**Risk Assessments**	**Access Management**	**Visibility and Analytics**	**Automation and Orchestration**	**Governance**
Initial	MFA has been implemented for authentication. **[SCORE=4]**	Identity management exists but is limited and not integrated. **[SCORE=2]**	Risk assessment is performed but remains static. **[SCORE=3]**	Access control is basic and not adaptive. **[SCORE=2]**	Limited visibility, no real-time identity analytics implemented. **[SCORE=1]**	Identity processes are manual/semi-automated and not orchestrated. **[SCORE=1]**	Governance exists at a basic level but is not risk-driven or fully enforced **[SCORE=1]**

Table 4. Maturity Score Pilar Device

Category	Identity (13/20)				Cross-Cutting capabilities		
Function	**Asset & Supply Chain Risk Management**	**Policy Enforcement & Compliance Monitoring**	**Resource Access**	**Device Threat Protection**	**Visibility and Analytics**	**Automation and Orchestration**	**Governance**
Initial	Asset inventory is mostly available, but supply chain risk is not fully managed. **[SCORE=3]**	Basic policies exist, but compliance monitoring is not continuous. **[SCORE=2]**	Device access to resources is controlled but not context-aware. **[SCORE=3]**	Threat protection exists at a basic level and is not integrated. **[SCORE=2]**	Limited visibility without real-time analytics. **[SCORE=1]**	No automation or orchestration in device management **[SCORE=1]**	Governance is minimal and not risk-based. **[SCORE=1]**

Table 5. Maturity Score Pilar Network

Category	Identity (11/20)				Cross-Cutting capabilities		
Function	**Network Segmentation**	**Network Traffic Management**	**Traffic Encryption**	**Network Resilience**	**Visibility and Analytics**	**Automation and Orchestration**	**Governance**
Traditional	Agency begins to adopt limited segmentation for critical workloads, but architecture still relies on macro segmentation and perimeter-based controls. Micro-segmentation and application-based policies are not yet implemented **[SCORE=2]**	Agency applies basic traffic rules and configurations, mostly static and manually managed. No dynamic or risk-based traffic prioritization is implemented. **[SCORE=2]**	Agency has implemented encryption for both internal and external communications with basic key management practices, but lacks enterprise-wide optimization and cryptographic agility **[SCORE=3]**	Network resilience is still reactive and limited. No adaptive mechanisms to dynamically handle workload changes or ensure service continuity. **[SCORE=1]**	Monitoring is based on limited indicators of compromise (IOC) and lacks centralized telemetry correlation across systems. No real-time analytics capability. **[SCORE=1]**	Network configuration and policy enforcement are mostly manual with minimal automation. No orchestration or automated change management processes are implemented. **[SCORE=1]**	Policies are static and perimeter-based, without dynamic enforcement or identity/application-based controls. Governance is not yet aligned with Zero Trust principles. **[SCORE=1]**

Table 6. Maturity Score Pilar Applications and Workloads

Category	Applications and Workloads (11/20)					Cross-Cutting capabilities		
Function	**Accessible Applications (Formerly Accessibility)**	**Secure Application Development and Deployment Workflow**	**Application Security Testing (Formerly Application Security)**	**Application Threat Protection (Formerly Threat Protections)**	**Application Access (Formerly Access Authorization)**	**Visibility and Analytics**	**Automation and Orchestration**	**Governance**
Traditional	Agency provides limited access to some mission-critical applications over network connections with basic protection mechanisms. Accessibility is still restricted and not fully optimized **[SCORE=1]**	Agency has begun separating development and production environments and applies basic controls, but secure development practices and CI/CD-based automation are not yet fully implemented. **[SCORE=2]**	Application security testing is conducted but still partial and largely manual, without full integration into the development lifecycle. **[SCORE=2]**	Application threat protection is minimal and applied generally, without deep integration into application workflows or advanced threat detection **[SCORE=1]**	Access control is implemented using basic authorization mechanisms, but lacks contextual and continuous authorization based on risk or behavior. **[SCORE=2]**	Monitoring is limited and not yet integrated across applications; lacks comprehensive visibility and real-time analytics. **[SCORE=1]**	Automation in application configuration and deployment is minimal, with most processes still manual and not orchestrated. **[SCORE=1]**	Governance relies on basic policies and manual enforcement, without integration into DevSecOps or automated policy control. **[SCORE=1]**

Table 7. Maturity Score Pilar Data

Category	Data (11/20)					Cross-Cutting capabilities		
Function	**Data Inventory Management**	**Data Categorization**	**Data Availability**	**Data Encryption**	**Data Access**	**Visibility and Analytics**	**Automation and Orchestration**	**Governance**
Traditional	Agency has basic data inventory practices and partial visibility of data assets, but inventory is not fully comprehensive or continuously updated. **[SCORE=2]**	Data classification and labeling are performed manually and inconsistently, lacking automation and dynamic sensitivity adjustment. **[SCORE=1]**	Data is available to users based on basic needs, but lacks dynamic access mechanisms and contextual controls. **[SCORE=1]**	Agency implements encryption for certain data at rest and in transit, but not consistently applied across all data environments. **[SCORE=2]**	Access to data is controlled using static policies without dynamic, risk-based, or context-aware access control. **[SCORE=2]**	Monitoring of data access and usage is limited, without integrated analytics or real-time visibility into data activities. **[SCORE=1]**	Data management processes are mostly manual with minimal automation in classification, protection, or access control. **[SCORE=1]**	Governance policies exist but are basic, static, and not fully aligned with data-centric Zero Trust principles **[SCORE=1]**

Volume 10, Number 02, Page 1045-1050
e-ISSN: 2598-120X; p-ISSN: 2598-117X

IV. CONCLUSIONS

Based on the results of the evaluation of the maturity level of Zero Trust implementation, PT XYZ obtained a maturity score of 60 out of a maximum of 100, which placed the organization at the Initial level. This achievement shows that organizations have adopted the basic principles of Zero Trust across all key pillars, namely Identity, Devices, Networks, Applications and Workloads, and Data. However, the implementation is still partial and has not been fully integrated, and has not been supported by adequate automation and analytics capabilities. When associated with the CISA Zero Trust Maturity Model (ZTMM) framework, this condition indicates that PT XYZ has surpassed the Traditional phase, but still has a significant gap to reach the Optimal level. The gap mainly lies in the lack of optimal implementation of continuous verification, dynamic policy enforcement, and cross-pillar integration needed to form adaptive and contextual security policies. Overall, the results of the assessment confirm that PT XYZ already has an initial foundation in the implementation of Zero Trust. However, further improvements are needed, particularly in the areas of automation, cross-domain integration, and continuous analytics, to drive the transformation towards a higher level of maturity and comprehensively aligned with Zero Trust principles.

REFERENCES

[1] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," Dec. 01, 2023, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/e25121595.

[2] C. Manzano, G. Marquez, and H. Astudillo, "Quality Attributes for Zero Trust Architecture-Based Systems," in Proceedings - International Conference of the Chilean Computer Science Society, SCCC, IEEE Computer Society, 2024. doi: 10.1109/SCCC63879.2024.10767657.

[3] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," Comput. Secur., vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103412.

[4] Y. Ren, Z. Wang, P. K. Sharma, F. Alqahtani, A. Tolba, and J. Wang, "Zero Trust Networks: Evolution and Application from Concept to Practice," 2025, Tech Science Press. doi: 10.32604/cmc.2025.059170.

[5] M. Ilyas, M. Akal, and Q. Althebyan, "Maturity Model for Corporate Sector Based on Zero Trust Adoption," in 2024 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, Dec. 2024, pp. 1–7. doi: 10.1109/ICEET65156.2024.10913750.

[6] A. Dalal, "Designing Zero Trust Security Models to Protect Distributed Networks and Minimize Cyber Risks," 2021.

[7] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," Journal of Engineering Research and Reports, vol. 26, no. 2, pp. 215–228, Feb. 2024, doi: 10.9734/jerr/2024/v26i21083.

[8] CISA, "Zero Trust Maturity Model Version 2.0," 2023. [Online]. Available: http://www.cisa.gov/tlp/.

[9] S. Alnoaimi and A. Alomary, "Zero Trust Security: A Comprehensive Comparative Analysis of Zero Trust Maturity Models," in 2nd International Conference on IT Innovations and Knowledge Discovery, ITIKD 2024, Institute of Electrical and Electronics Engineers Inc., 2025. doi: 10.1109/ITIKD63574.2025.11005097.

[10] F. Santucci et al., "Implementing Zero Trust: Expert Insights on Key Security Pillars and Prioritization in Digital Transformation," Information (Switzerland), vol. 16, no. 8, Aug. 2025, doi: 10.3390/info16080667.

[11] V. Kalekar, "Advancing Zero Trust Maturity Assessment with a Quantitative Scoring System," in Proceedings of the IEEE International Conference on Computer Communication and the Internet, ICCCI, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 72–85. doi: 10.1109/ICCCI65070.2025.11158460.