Strategic Management of Zero-Trust Network Architecture Implementation in Large Organizations

Mohammad Ali. Haghighi[1*]

[1] MA, Department of Computer Engineering, Faculty of Computer Engineering, University of Science and Technology, Tehran, Iran

*** Corresponding author email address**: mhrce2020@gmail.com

Received: 2026-02-10 **Revised:** 2026-07-04 **Accepted:** 2026-07-11 **Initial Publish:** 2026-08-15 **Final Publish:** 2027-07-01

Abstract

This study aimed to develop and test a structural model explaining the direct and indirect effects of strategic alignment and executive commitment, governance and policy development, technological and infrastructural readiness, human resources and change management, and cybersecurity risk and compliance management on the effectiveness of zero-trust network architecture implementation in large organizations. This applied, quantitative, cross-sectional, descriptive-correlational study was conducted among 384 senior managers, information technology managers, cybersecurity specialists, network administrators, enterprise architects, and risk and governance professionals employed in large public and private organizations in Tehran, Iran. Participants were selected using proportional stratified and purposive sampling. Data were collected using a demographic form and the 48-item Strategic Management of Zero-Trust Architecture Implementation Questionnaire. The instrument measured six dimensions and demonstrated acceptable content validity, construct validity, internal consistency, convergent validity, and discriminant validity. Data were analyzed using descriptive statistics, Pearson correlation coefficients, confirmatory factor analysis, and partial least squares structural equation modeling in SPSS 27 and SmartPLS 4. All proposed direct and indirect paths were positive and statistically significant. Strategic alignment and executive commitment significantly predicted governance and policy development ($\beta = 0.58$, $p < 0.001$), technological and infrastructural readiness ($\beta = 0.37$, $p < 0.001$), and human resources and change management ($\beta = 0.44$, $p < 0.001$). Governance significantly predicted cybersecurity risk and compliance management ($\beta = 0.49$, $p < 0.001$). Technological readiness had the strongest direct effect on implementation effectiveness ($\beta = 0.30$, $p < 0.001$), followed by governance ($\beta = 0.22$, $p < 0.001$), cybersecurity risk management ($\beta = 0.21$, $p < 0.001$), human resources and change management ($\beta = 0.19$, $p < 0.001$), and strategic alignment ($\beta = 0.14$, $p = 0.003$). The model explained 68.3% of the variance in implementation effectiveness. Effective zero-trust implementation depends on the coordinated development of executive leadership, formal governance, technological readiness, workforce adaptation, and risk-management capability rather than on isolated security technologies.

Keywords: *Zero-trust architecture; strategic management; cybersecurity governance; technological readiness; change management; structural equation modeling.*

How to cite this article:

Haghighi, M. A. (2027). Design of a Fuzzy Multi-Objective Mathematical Model for Short-Term Preventive Maintenance Scheduling Using a Total Productive Maintenance Approach. Management Strategies and Engineering Sciences, 9(4), 1-19.

1. Introduction

The accelerating digitalization of organizational processes has fundamentally altered the structure, scope, and strategic significance of enterprise cybersecurity. Large organizations increasingly depend on cloud services, distributed applications, mobile workforces, third-party platforms, interconnected operational technologies, and data-intensive decision systems. Although these developments create considerable opportunities for organizational agility and innovation, they also dissolve the traditional boundaries that once separated trusted internal networks from untrusted external environments. Conventional perimeter-based security models generally assume that users, devices, and applications located inside the organizational network can be trusted after passing an initial authentication checkpoint. This assumption has become increasingly difficult to justify because

compromised credentials, insider threats, remote access, cloud-based resources, supply-chain dependencies, and lateral movement by attackers can expose critical assets even when the external perimeter remains technically intact. Zero-trust network architecture has emerged in response to these conditions as a security paradigm based on continuous verification, least-privilege access, explicit authorization, contextual evaluation, and the principle that no user, device, workload, or network location should be trusted by default [1, 2].

Zero trust is not merely a collection of security products or a replacement for a specific network-control mechanism. It represents a comprehensive architectural and managerial approach in which access decisions are continuously informed by identity, device condition, resource sensitivity, behavioral context, environmental risk, and organizational policy. Under this approach, trust is treated as temporary, conditional, and continuously reassessed rather than permanently granted after entry into the network. Guidance concerning secure enterprise network landscapes has emphasized the need to integrate identity systems, endpoint controls, access gateways, segmentation mechanisms, monitoring capabilities, and policy-enforcement components across heterogeneous organizational environments [3, 4]. Planning for zero-trust architecture therefore requires organizations to identify critical assets, map data flows, determine access requirements, define trust boundaries, establish policy-decision and enforcement mechanisms, and progressively improve security maturity rather than attempting an immediate organization-wide replacement of existing infrastructure [5]. Consequently, the implementation of zero trust should be understood as a strategic transformation program involving technology, governance, human resources, risk management, investment prioritization, and organizational change.

The growing importance of zero trust has generated a substantial body of research addressing its principles, architectures, applications, and implementation challenges. Reviews of the field have shown that zero-trust models commonly incorporate continuous authentication, identity-centric access management, micro-segmentation, least-privilege authorization, real-time monitoring, encryption, security analytics, and policy automation [6, 7]. Comparative assessments have further demonstrated that zero-trust approaches differ in their architectural assumptions, policy models, implementation technologies, scalability, interoperability, and suitability for particular organizational domains [8]. More recent comprehensive reviews have traced the evolution of zero trust from an alternative network-security concept to a multidimensional enterprise architecture intended to protect users, devices, applications, workloads, and data across hybrid environments [9]. Systematic evidence also indicates that implementation challenges recur across sectors, including legacy-system incompatibility, cost, operational complexity, limited expertise, integration difficulties, policy fragmentation, performance concerns, and resistance to organizational change [10]. These findings suggest that the effectiveness of zero trust cannot be explained solely by the technical quality of its individual components.

The need for a strategic perspective becomes especially evident in large organizations. Such organizations typically possess complex reporting structures, multiple business units, extensive application portfolios, heterogeneous networks, accumulated technical debt, distributed data ownership, and diverse regulatory obligations. A zero-trust initiative introduced without clear strategic alignment may become fragmented across departments, implemented as a narrow information technology project, or reduced to the acquisition of isolated security tools. Strategic alignment is therefore required to connect zero-trust objectives with enterprise risk appetite, digital-transformation priorities, business continuity, operational resilience, data protection, and long-term organizational performance. Executive commitment is equally important because the transition may require significant financial resources, cross-functional authority, modification of established workflows, and sustained support across multiple implementation phases. Debates concerning whether zero trust is an effective security transformation or an overpromoted solution reinforce the importance of realistic executive expectations and context-sensitive implementation decisions [11]. Developments characterized as Zero Trust 2.0 likewise emphasize that the future of the model depends on advances in automation, adaptive policy, intelligent analytics, interoperability, and governance rather than on the simple repetition of the “never trust” principle [12].

Governance and policy development constitute another central dimension of strategic zero-trust management. Zero-trust controls must be supported by formal policies specifying who may access which resources, under what circumstances, from which devices, for what purposes, and for how long. Governance arrangements are needed to assign decision rights, establish accountability, coordinate information technology and business units, define ownership of identities and data, and monitor compliance with

organizational standards. Without such arrangements, different departments may interpret zero trust inconsistently, create incompatible access rules, or introduce exceptions that weaken the overall security model. Research concerning the deployment of zero-trust access policies has highlighted the value of explicit access-control rules for protecting users and network infrastructure from unauthorized activity [13]. Similarly, cloud-native and multi-location environments require access-control models capable of maintaining consistent policy across distributed applications and infrastructures [14]. Governance is therefore the mechanism through which high-level strategic commitment is converted into enforceable rules, coordinated responsibilities, measurable objectives, and operational accountability.

Technological and infrastructural readiness remains indispensable because zero-trust principles must ultimately be implemented through functional enterprise capabilities. These capabilities may include identity and access management, multifactor authentication, privileged-access control, endpoint detection, device-health assessment, software-defined perimeters, network and application segmentation, data classification, encryption, security information and event management, user and entity behavior analytics, and automated policy enforcement. In cloud environments, implementation is complicated by shared responsibility, dynamic resources, multi-cloud configurations, application programming interfaces, and the need to maintain consistent visibility across rapidly changing workloads [15, 16]. Research on Microsoft Azure environments has shown that practical implementation requires careful integration of identity services, conditional access, monitoring, cloud-security tools, and organizational processes rather than reliance on a single platform feature [17]. Likewise, zero-trust designs for large data platforms demonstrate the importance of integrating architecture with the characteristics of organizational information resources and operational requirements [18]. Accordingly, infrastructural readiness concerns not only the availability of advanced technology but also compatibility, scalability, interoperability, data quality, and the ability to integrate new controls with legacy systems.

Automation and intelligent analytics have become increasingly relevant to this technological dimension. Continuous verification can generate large volumes of authentication events, device signals, network telemetry, and behavioral data that cannot be evaluated effectively through manual procedures alone. Automation and orchestration can support rapid policy enforcement, access revocation, incident containment, and coordinated responses across security tools; however, they also create challenges related to integration, explainability, false positives, policy conflicts, and operational governance [19]. Machine-learning-based zero-trust frameworks have sought to combine security information and event management, security orchestration and automated response, and user and entity behavior analytics to provide context-aware threat mitigation [20]. Artificial intelligence has also been proposed as a means of strengthening cloud security in environments involving large language models and other systems whose internal decision processes may be difficult to interpret [21]. These developments increase the potential responsiveness of zero-trust environments, but they simultaneously strengthen the need for strategic oversight because automated access decisions can affect employee productivity, service availability, legal compliance, and organizational accountability.

The human and organizational dimensions of implementation are no less important than infrastructure. Zero trust changes how employees, administrators, contractors, managers, and external partners interact with organizational resources. Users may face additional authentication requirements, restricted permissions, device-compliance checks, changes in remote-access procedures, and continuous monitoring of activity. When these changes are introduced without adequate communication and training, employees may perceive zero trust as an obstacle to their work or as an expression of managerial distrust. Technical personnel may also resist the architecture when it increases administrative burdens, exposes deficiencies in existing systems, or redistributes decision-making authority among departments. Migration research has therefore emphasized that zero-trust adoption is a progressive process requiring assessment, planning, prioritization, implementation, monitoring, and continuous refinement [22]. A comprehensive migration framework similarly underscores the importance of evaluating organizational readiness, establishing phased implementation roadmaps, identifying dependencies, and adapting the architecture to the organization's existing security maturity [23]. Effective change management must consequently include stakeholder participation, role-specific training, communication of strategic benefits, management of resistance, and support for new patterns of secure behavior.

Legacy environments present a particularly significant organizational and technical barrier. Large enterprises often depend on applications, devices, and industrial systems that

were not designed for continuous authentication, fine-grained authorization, or modern identity integration. This challenge is prominent in manufacturing environments, where operational continuity, safety, real-time performance, and long equipment life cycles can restrict the replacement or modification of existing systems. Research on implementing zero trust in legacy industrial environments indicates that organizations must balance security transformation with operational feasibility, resource constraints, and the characteristics of industrial technology [24]. The convergence of cloud systems with industrial operational-technology networks further expands the attack surface and creates new dependencies between information technology and physical operations [25]. These conditions require strategic sequencing, compensating controls, asset prioritization, and careful testing so that security improvements do not create unacceptable interruptions to essential organizational activities.

Zero-trust implementation must also be closely connected to cybersecurity risk and compliance management. From a risk-management perspective, the architecture is intended to reduce the probability and potential impact of unauthorized access, credential compromise, lateral movement, data leakage, and persistent intrusion. Its value therefore depends on whether controls are selected and prioritized according to asset criticality, threat exposure, vulnerability, business impact, and regulatory obligation. Research has conceptualized zero-trust architecture as a risk countermeasure that can strengthen security in small and medium-sized enterprises as well as advanced technology systems, while also emphasizing the need to consider implementation costs and organizational context [26]. Zero-trust strategies are particularly relevant to advanced persistent threats because such threats frequently exploit valid credentials, maintain long-term access, and move gradually across organizational networks [27]. Risk-based implementation allows organizations to focus initial efforts on high-value assets, privileged identities, sensitive data, critical applications, and external access points instead of applying identical controls indiscriminately across all resources.

Sector-specific studies illustrate how zero trust must be aligned with different threat environments and strategic priorities. In banking, zero-trust models have been combined with blockchain-based consensus mechanisms to address data breaches, integrity risks, and distributed trust requirements [28]. Distributed financial applications additionally require secure management of secrets, credentials, cryptographic keys, and service identities, making vault-based secret management an important component of a broader zero-trust model [29]. In fifth-generation communication systems, researchers have examined zero-trust principles at the air-interface level, demonstrating that trust decisions may extend beyond conventional enterprise access and into telecommunications architecture [30]. Communication, navigation, and surveillance systems involve further requirements related to availability, mission assurance, heterogeneous devices, and operational continuity [31]. These examples demonstrate that zero trust is not a uniform template; rather, its strategic management must account for the organization's industry, operational dependencies, regulatory environment, technology profile, and risk tolerance.

Emerging applications also show that zero-trust principles are being extended into decentralized, collaborative, autonomous, and resource-constrained environments. Proposals for decentralized zero-trust operationalization seek to reduce dependence on centralized control points and support distributed policy enforcement across complex systems [32]. Activity-control models for smart collaborative environments similarly emphasize the need for dynamic security policies that respond to ongoing actions rather than relying exclusively on static permissions [33]. In networks of unmanned aerial vehicles and Internet of Battlefield Things environments, zero-trust architecture must address mobility, intermittent connectivity, device constraints, adversarial conditions, and highly dynamic trust relationships [34]. Device-authentication frameworks using mechanisms such as quantum fingerprinting further demonstrate the search for resilient methods of verifying devices that request network access [35]. A semiotic approach to network security also suggests that access and threat evaluation may benefit from richer interpretation of signals, indicators, and contextual meanings within a security environment [36]. Although these developments are technologically diverse, all require strategic decisions concerning control distribution, policy authority, interoperability, and acceptable operational risk.

Despite the expansion of the literature, much of the existing research remains primarily technical, architectural, or domain-specific. Studies frequently describe components, propose frameworks, compare security mechanisms, or examine implementation within a particular platform or operational setting. These contributions are essential, but they provide limited empirical explanation of how managerial and organizational capabilities interact to

determine implementation effectiveness in large organizations. In particular, insufficient attention has been paid to the relationships among strategic alignment and executive commitment, governance and policy development, technological and infrastructural readiness, human resources and organizational change, and cybersecurity risk and compliance management. The strategic management of zero trust requires these dimensions to operate as an integrated system. Executive commitment can strengthen governance, authorize investment, and support organizational change; governance can translate strategic priorities into policy and accountability; technological readiness can enable continuous verification and control enforcement; human-resource capabilities can support adoption and reduce resistance; and risk management can ensure that implementation priorities reflect actual organizational exposure. The effectiveness of implementation should therefore be assessed as the result of coordinated strategic capabilities rather than as the outcome of isolated technical controls.

A further gap concerns the empirical examination of indirect pathways. Strategic leadership may influence implementation effectiveness directly, but much of its practical effect is likely to occur through stronger governance, improved infrastructure, and more effective change management. Governance may similarly affect outcomes both directly and indirectly by improving cybersecurity risk and compliance management. Without testing these relationships simultaneously, organizations may overestimate the importance of technology acquisition while underestimating the enabling roles of leadership, policy, personnel, and risk-based coordination. This issue is especially important in large organizations in rapidly developing digital environments, where substantial investment in cybersecurity does not necessarily produce integrated implementation. An empirically tested structural model can clarify which capabilities exert the strongest direct effects, which operate as upstream strategic drivers, and which mediate the relationship between executive intent and implementation outcomes.

Accordingly, the aim of this study was to develop and empirically test a structural model of the direct and indirect effects of strategic alignment and executive commitment, governance and policy development, technological and infrastructural readiness, human resources and change management, and cybersecurity risk and compliance management on the effectiveness of zero-trust network architecture implementation in large organizations in Tehran.

2. Methodology

This applied study employed a quantitative, cross-sectional, descriptive-correlational design to examine the strategic, organizational, technological, and managerial factors associated with the successful implementation of zero-trust network architecture in large organizations. The statistical population consisted of senior managers, information technology managers, chief information officers, cybersecurity managers, network administrators, information security specialists, enterprise architects, risk-management experts, and information technology governance professionals working in large public and private organizations located in Tehran, Iran. For the purposes of this study, a large organization was defined as an organization employing at least 250 personnel and maintaining an independent information technology or information security unit. The participating organizations operated in the banking and financial services, telecommunications, governmental services, healthcare, insurance, energy, manufacturing, and technology sectors. The minimum required sample size was estimated using Cochran's formula for a large population, with a confidence level of 95%, a margin of error of 5%, and maximum population variability. Accordingly, 384 participants were included in the final sample. To ensure adequate representation of different organizational environments, proportional stratified sampling was initially used to classify the organizations according to their sector, after which eligible participants were selected through purposive sampling within each stratum. The inclusion criteria were employment in a large organization in Tehran, possession of at least a bachelor's degree in management, information technology, computer engineering, cybersecurity, industrial engineering, or a related field, a minimum of three years of professional experience in information technology management, information security, network administration, strategic planning, organizational risk management, or digital transformation, and familiarity with network-security policies or zero-trust principles. Participants who returned substantially incomplete questionnaires, provided patterned or inconsistent responses, or lacked direct involvement in organizational technology or security decision-making were excluded from the analysis. Data collection was conducted through both electronic and paper-based questionnaires

distributed with the authorization of the participating organizations. Before completing the questionnaire, all participants were informed about the objectives of the study, the voluntary nature of participation, the confidentiality of their information, and their right to withdraw from the study at any stage. No personally identifiable information was collected, and all responses were analyzed in aggregate form.

Data were collected using a demographic and professional information form and the Strategic Management of Zero-Trust Architecture Implementation Questionnaire. The demographic and professional information form was developed to obtain information regarding participants' age, gender, educational level, academic specialization, organizational position, years of professional experience, field of activity, organization type, organization size, level of involvement in cybersecurity decision-making, and previous experience with zero-trust technologies. The Strategic Management of Zero-Trust Architecture Implementation Questionnaire was developed by the researchers based on the conceptual foundations of zero-trust architecture, strategic information systems management, organizational readiness, technology governance, cybersecurity risk management, and organizational change management. The initial item pool was generated following a comprehensive review of the relevant theoretical literature, zero-trust implementation frameworks, enterprise-security guidelines, and strategic-management models. The preliminary questionnaire contained 62 items, which were reviewed by a panel of 12 experts in strategic management, information technology governance, cybersecurity, network architecture, organizational behavior, and digital transformation. Based on the experts' evaluations of the relevance, clarity, necessity, and comprehensiveness of the items, redundant, ambiguous, or conceptually overlapping statements were revised or removed. The final questionnaire consisted of 48 items organized into six dimensions: strategic alignment and executive commitment, governance and policy development, technological and infrastructural readiness, human resources and organizational change management, cybersecurity risk and compliance management, and zero-trust implementation effectiveness. The strategic alignment and executive commitment dimension included eight items assessing the extent to which zero-trust initiatives were connected to organizational objectives, supported by senior management, and incorporated into strategic planning. The governance and policy development dimension contained eight items measuring role clarity, accountability, access-control policies, data governance, interdepartmental coordination, and the formalization of zero-trust procedures. The technological and infrastructural readiness dimension comprised nine items evaluating identity and access-management capabilities, network segmentation, device visibility, continuous authentication, data classification, legacy-system compatibility, monitoring capacity, automation, and security analytics. The human resources and organizational change-management dimension included eight items examining employee awareness, technical competence, resistance to change, training, communication, participation, and managerial support during implementation. The cybersecurity risk and compliance-management dimension consisted of seven items assessing risk identification, regulatory compliance, incident-response readiness, third-party access control, continuous risk assessment, and the integration of zero-trust practices with enterprise risk-management processes. The zero-trust implementation-effectiveness dimension contained eight items measuring improvements in access control, threat detection, incident containment, protection of sensitive information, operational resilience, regulatory compliance, and the overall achievement of implementation objectives.

All questionnaire items were scored on a five-point Likert scale ranging from 1, representing "strongly disagree," to 5, representing "strongly agree." Higher scores indicated stronger strategic-management capabilities, greater organizational readiness, and more effective implementation of zero-trust network architecture. The total score was calculated by summing the scores of all items, while dimension-specific scores were obtained by calculating the mean of the items associated with each construct. Content validity was evaluated using the content validity ratio and content validity index. Items that did not meet the acceptable quantitative criteria or were considered unclear by the expert panel were revised or eliminated. Face validity was also examined through interviews with eight professionals from the target population to determine whether the wording, structure, and technical terminology of the questionnaire were understandable and appropriate for the organizational context. Before the main data collection phase, the instrument was administered to a pilot sample of 40 information technology and cybersecurity professionals who were not included in the final sample. The internal consistency of the questionnaire and its dimensions was assessed using Cronbach's alpha and composite reliability coefficients, with values of 0.70 or higher considered

acceptable. Construct validity was evaluated through confirmatory factor analysis by examining standardized factor loadings, average variance extracted, composite reliability, convergent validity, and discriminant validity. The final measurement model demonstrated satisfactory psychometric properties, indicating that the questionnaire was suitable for evaluating the strategic management of zero-trust architecture implementation in large organizations.

The collected data were analyzed using IBM SPSS Statistics version 27 and SmartPLS version 4. Before conducting the main analyses, the dataset was screened for incomplete responses, data-entry errors, univariate and multivariate outliers, patterned answers, and missing values. Questionnaires with substantial missing information or evidence of invalid response patterns were excluded. Descriptive statistics, including frequency, percentage, mean, standard deviation, minimum, maximum, skewness, and kurtosis, were calculated to summarize participants' demographic characteristics and the distribution of the research variables. The normality of the variables was examined using skewness and kurtosis indices, histograms, and the Kolmogorov–Smirnov test. Pearson correlation coefficients were calculated to determine the direction and magnitude of the relationships among the main study variables. Because the study focused on predicting zero-trust implementation effectiveness and simultaneously examining relationships among several strategic, organizational, and technological constructs, partial least squares structural equation modeling was employed.

The measurement model was evaluated before testing the structural relationships. Indicator reliability was examined using standardized factor loadings, and items with weak loadings were reviewed with consideration of their theoretical importance and their effects on construct reliability and validity. Internal consistency was assessed using Cronbach's alpha, rho_A, and composite reliability. Convergent validity was evaluated through the average variance extracted, with values above 0.50 considered acceptable. Discriminant validity was assessed using the Fornell–Larcker criterion, cross-loadings, and the heterotrait–monotrait ratio. The structural model was subsequently evaluated by examining variance inflation factor values to identify potential multicollinearity, standardized path coefficients to determine the direction and strength of the hypothesized relationships, coefficients of determination to assess the explanatory power of the model, effect-size coefficients to determine the contribution of each predictor, and Stone–Geisser predictive-relevance values to assess the model's predictive capability. The statistical significance of the direct and indirect effects was determined through a bootstrapping procedure with 5,000 resamples. The standardized root mean square residual was also used as an indicator of approximate model fit. Mediation effects were examined when organizational readiness, governance quality, or change-management capability was hypothesized to transmit the effects of strategic-management factors to implementation effectiveness. A significance level of 0.05 was adopted for all statistical tests, and the findings were reported using standardized coefficients, test statistics, probability values, confidence intervals, effect sizes, and explained variance.

3. Findings and Results

A total of 384 completed questionnaires were included in the final analysis. Of the participants, 271 individuals were men (70.6%) and 113 were women (29.4%). Regarding age, 48 participants (12.5%) were younger than 30 years, 134 participants (34.9%) were between 30 and 39 years, 128 participants (33.3%) were between 40 and 49 years, and 74 participants (19.3%) were 50 years of age or older. The mean age of the participants was 40.72 years, with a standard deviation of 8.31 years. In terms of educational attainment, 142 participants (37.0%) held a bachelor's degree, 185 participants (48.2%) held a master's degree, and 57 participants (14.8%) held a doctoral degree. Regarding professional experience, 65 participants (16.9%) had between 3 and 5 years of experience, 106 participants (27.6%) had between 6 and 10 years of experience, 108 participants (28.1%) had between 11 and 15 years of experience, and 105 participants (27.3%) had more than 15 years of professional experience. The mean professional experience of the sample was 12.46 years, with a standard deviation of 6.27 years.

With respect to organizational positions, 89 participants (23.2%) were senior information technology managers or chief information officers, 112 participants (29.2%) were cybersecurity managers or information-security specialists, 86 participants (22.4%) were network administrators or enterprise architects, 57 participants (14.8%) were information technology governance, compliance, or risk-management professionals, and 40 participants (10.4%) were senior organizational managers involved in strategic technology decision-making. Seventy-four participants (19.3%) were employed in banking and financial-service

organizations, 69 participants (18.0%) worked in governmental and public-service organizations, 66 participants (17.2%) were employed in telecommunications and technology organizations, 58 participants (15.1%) worked in healthcare and insurance organizations, 72 participants (18.8%) were employed in energy and manufacturing organizations, and 45 participants (11.7%) worked in other large service organizations. In addition, 241 participants (62.8%) were employed in private-sector organizations, while 143 participants (37.2%) worked in public or state-affiliated organizations. A total of 293 participants (76.3%) reported direct involvement in cybersecurity or information technology governance decisions, and 91 participants (23.7%) reported an advisory or operational role in such decisions. Furthermore, 246 participants (64.1%) indicated that their organizations had initiated or partially implemented at least one component of zero-trust architecture, whereas 138 participants (35.9%) reported that their organizations were still at the assessment, planning, or preliminary preparation stage.

Table 1. Descriptive Statistics and Correlations Among the Study Variables

Variable	Mean	SD	Minimum	Maximum	Skewness	Kurtosis	1	2	3	4	5	6
1. Strategic alignment and executive commitment	3.68	0.71	1.63	5.00	−0.31	−0.18	1.00					
2. Governance and policy development	3.51	0.73	1.38	5.00	−0.24	−0.27	0.62	1.00				
3. Technological and infrastructural readiness	3.42	0.76	1.22	5.00	−0.18	−0.35	0.57	0.63	1.00			
4. Human resources and change management	3.29	0.79	1.13	5.00	−0.09	−0.42	0.54	0.58	0.56	1.00		
5. Cybersecurity risk and compliance management	3.57	0.70	1.43	5.00	−0.27	0.08	0.60	0.66	0.61	0.55	1.00	
6. Zero-trust implementation effectiveness	3.46	0.74	1.25	5.00	−0.21	−0.12	0.65	0.70	0.72	0.66	0.69	1.00

As presented in Table 1, the highest mean score was obtained for strategic alignment and executive commitment, with a mean of 3.68 and a standard deviation of 0.71. This finding indicated that senior-management support, strategic recognition of cybersecurity, and alignment of zero-trust initiatives with organizational objectives were relatively more developed than the other examined dimensions. Cybersecurity risk and compliance management had the second-highest mean score, with a mean of 3.57 and a standard deviation of 0.70, followed by governance and policy development, with a mean of 3.51 and a standard deviation of 0.73. The mean score for zero-trust implementation effectiveness was 3.46, indicating that the participating organizations had achieved a moderate-to-relatively-high level of effectiveness in implementing zero-trust principles. Technological and infrastructural readiness had a mean score of 3.42, whereas human resources and organizational change management produced the lowest mean score, at 3.29. The relatively lower score for human resources and change management suggested that employee preparation, specialized training, communication, cultural adaptation, and resistance-management mechanisms were less developed than strategic, technical, and governance-related arrangements.

The skewness values ranged from −0.31 to −0.09, while the kurtosis values ranged from −0.42 to 0.08. These values were within acceptable limits and did not indicate substantial univariate non-normality. Examination of the correlations demonstrated that all study variables were positively and significantly related to one another. Zero-trust implementation effectiveness had its strongest bivariate relationship with technological and infrastructural readiness, with a correlation coefficient of 0.72, followed by governance and policy development, with a correlation coefficient of 0.70, and cybersecurity risk and compliance management, with a correlation coefficient of 0.69. The relationship between human resources and change management and implementation effectiveness was also positive and relatively strong, at 0.66. Strategic alignment and executive commitment had a positive correlation of 0.65 with implementation effectiveness. These findings provided preliminary evidence that the effectiveness of zero-trust implementation was not exclusively dependent on technical infrastructure but was simultaneously associated with strategic leadership, governance arrangements, human-resource preparation, and cybersecurity risk-management capabilities. Although several relationships were relatively strong, none of the correlation coefficients exceeded 0.80,

indicating that the constructs were related but did not appear to represent redundant organizational capabilities.

Table 2. Reliability and Convergent Validity of the Measurement Model

Construct	Number of Items	Standardized Loading Range	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted
Strategic alignment and executive commitment	8	0.71–0.88	0.90	0.91	0.92	0.60
Governance and policy development	8	0.70–0.87	0.89	0.90	0.92	0.58
Technological and infrastructural readiness	9	0.70–0.86	0.91	0.92	0.93	0.60
Human resources and change management	8	0.70–0.85	0.88	0.89	0.91	0.56
Cybersecurity risk and compliance management	7	0.72–0.89	0.89	0.90	0.92	0.62
Zero-trust implementation effectiveness	8	0.73–0.90	0.92	0.93	0.94	0.66

The measurement-model results reported in Table 2 supported the reliability and convergent validity of the six study constructs. The standardized factor loadings ranged from 0.70 to 0.90, and all loadings were statistically significant at $p < 0.001$. The highest indicator loading was observed within the zero-trust implementation-effectiveness construct, whereas the lowest acceptable loading was 0.70. Because all indicator loadings met or exceeded the minimum acceptable level and were theoretically consistent with their assigned constructs, no item was removed from the final measurement model. The Cronbach's alpha coefficients ranged from 0.88 for human resources and change management to 0.92 for zero-trust implementation effectiveness. Therefore, all constructs exceeded the minimum internal-consistency criterion of 0.70 and demonstrated satisfactory to excellent reliability.

The rho_A coefficients ranged from 0.89 to 0.93, further confirming the stability and internal consistency of the measurement scales. Composite reliability values ranged from 0.91 to 0.94, indicating that the indicators associated with each latent construct consistently measured the same underlying concept. The composite reliability coefficient for zero-trust implementation effectiveness was the highest, at 0.94, followed by technological and infrastructural readiness, at 0.93. The composite reliability coefficients for strategic alignment and executive commitment, governance and policy development, and cybersecurity risk and compliance management were each 0.92, while the coefficient for human resources and change management was 0.91. These values were below the threshold at which excessive item redundancy would be suspected and therefore demonstrated adequate construct reliability without indicating problematic duplication among the questionnaire items.

The average variance extracted values ranged from 0.56 to 0.66 and were above the recommended threshold of 0.50 for every construct. Thus, each latent variable explained more than half of the variance in its observed indicators. Zero-trust implementation effectiveness had the highest average variance extracted, at 0.66, indicating that its indicators shared a particularly strong proportion of common variance. Cybersecurity risk and compliance management had an average variance extracted of 0.62, while strategic alignment and executive commitment and technological and infrastructural readiness each had an average variance extracted of 0.60. Governance and policy development had a value of 0.58, and human resources and change management had a value of 0.56. Collectively, the standardized factor loadings, Cronbach's alpha coefficients, rho_A coefficients, composite reliability values, and average variance extracted values confirmed that the measurement model possessed acceptable indicator reliability, internal consistency, and convergent validity. The instrument was therefore considered sufficiently reliable and valid for evaluating the structural relationships among the strategic-management dimensions and zero-trust implementation effectiveness.

Table 3. Heterotrait–Monotrait Ratios for Assessment of Discriminant Validity

Construct	1	2	3	4	5	6
1. Strategic alignment and executive commitment	—					
2. Governance and policy development	0.70	—				
3. Technological and infrastructural readiness	0.64	0.71	—			
4. Human resources and change management	0.61	0.65	0.63	—		
5. Cybersecurity risk and compliance management	0.68	0.74	0.69	0.62	—	
6. Zero-trust implementation effectiveness	0.72	0.79	0.81	0.74	0.77	—

The discriminant-validity results presented in Table 3 demonstrated that the heterotrait–monotrait ratios ranged from 0.61 to 0.81. All values were below the conservative criterion of 0.85, indicating that each construct was empirically distinguishable from the other constructs included in the model. The highest heterotrait–monotrait ratio, 0.81, was observed between technological and infrastructural readiness and zero-trust implementation effectiveness. This relatively strong value was theoretically expected because the effectiveness of zero-trust architecture depends substantially on technological capabilities such as identity and access management, network segmentation, device visibility, continuous authentication, security analytics, and automated monitoring. Nevertheless, the value remained below the specified threshold, demonstrating that technological readiness and implementation effectiveness were not statistically interchangeable concepts.

The heterotrait–monotrait ratio between governance and policy development and zero-trust implementation effectiveness was 0.79, while the ratio between cybersecurity risk and compliance management and implementation effectiveness was 0.77. Human resources and change management had a heterotrait–monotrait ratio of 0.74 with implementation effectiveness, and strategic alignment and executive commitment had a corresponding value of 0.72. Among the predictor constructs, the highest ratio was observed between governance and policy development and cybersecurity risk and compliance management, at 0.74. This result reflected the conceptual relationship between formal security governance and the organizational management of cyber risks and regulatory requirements, but it remained sufficiently low to support the distinctiveness of the two constructs.

The Fornell–Larcker criterion also supported discriminant validity. The square roots of the average variance extracted values were 0.775 for strategic alignment and executive commitment, 0.762 for governance and policy development, 0.775 for technological and infrastructural readiness, 0.748 for human resources and change management, 0.787 for cybersecurity risk and compliance management, and 0.812 for zero-trust implementation effectiveness. Each of these values was greater than the corresponding correlations between the relevant construct and the other latent variables. Furthermore, examination of the indicator cross-loadings showed that every item loaded more strongly on its intended construct than on the remaining constructs. Therefore, the heterotrait–monotrait ratios, Fornell–Larcker results, and cross-loading patterns jointly confirmed satisfactory discriminant validity.

Before evaluating the structural paths, collinearity among the predictor variables was assessed using variance inflation factor values. The inner variance inflation factors ranged from 1.64 to 2.83, which were below the critical threshold of 3.30. Thus, multicollinearity did not represent a serious concern, and the estimated path coefficients could be interpreted without evidence that excessive overlap among the predictors had substantially distorted the model. The standardized root mean square residual was 0.058, which was below the recommended value of 0.08 and indicated an acceptable approximate model fit. The normed fit index was 0.912, providing additional support for the adequacy of the proposed model. These findings demonstrated that both the measurement structure and the overall specification of the model were sufficiently acceptable to proceed with structural-model testing.

Table 4. Direct and Indirect Effects in the Structural Model

Structural Relationship	Standardized β	SE	t	p	95% Bootstrap Confidence Interval	f^2	Result
Strategic alignment and executive commitment → Governance and policy development	0.58	0.041	14.15	<0.001	0.498 to 0.658	0.50	Significant
Strategic alignment and executive commitment → Technological and infrastructural readiness	0.37	0.046	8.04	<0.001	0.278 to 0.456	0.16	Significant
Strategic alignment and executive commitment → Human resources and change management	0.44	0.044	10.00	<0.001	0.352 to 0.523	0.24	Significant
Governance and policy development → Cybersecurity risk and compliance management	0.49	0.043	11.40	<0.001	0.405 to 0.573	0.32	Significant
Strategic alignment and executive commitment → Zero-trust implementation effectiveness	0.14	0.047	2.98	0.003	0.049 to 0.232	0.03	Significant
Governance and policy development → Zero-trust implementation effectiveness	0.22	0.052	4.23	<0.001	0.119 to 0.321	0.07	Significant
Technological and infrastructural readiness → Zero-trust implementation effectiveness	0.30	0.049	6.12	<0.001	0.205 to 0.396	0.14	Significant
Human resources and change management → Zero-trust implementation effectiveness	0.19	0.044	4.32	<0.001	0.103 to 0.275	0.08	Significant
Cybersecurity risk and compliance management → Zero-trust implementation effectiveness	0.21	0.050	4.20	<0.001	0.111 to 0.309	0.08	Significant
Strategic alignment and executive commitment → Governance and policy development → Zero-trust implementation effectiveness	0.128	0.034	3.76	<0.001	0.067 to 0.198	—	Significant
Strategic alignment and executive commitment → Technological and infrastructural readiness → Zero-trust implementation effectiveness	0.111	0.029	3.83	<0.001	0.059 to 0.171	—	Significant
Strategic alignment and executive commitment → Human resources and change management → Zero-trust implementation effectiveness	0.084	0.024	3.50	<0.001	0.043 to 0.136	—	Significant
Governance and policy development → Cybersecurity risk and compliance management → Zero-trust implementation effectiveness	0.103	0.031	3.32	0.001	0.050 to 0.170	—	Significant
Strategic alignment and executive commitment → Governance and policy development → Cybersecurity risk and compliance management → Zero-trust implementation effectiveness	0.060	0.021	2.86	0.004	0.025 to 0.107	—	Significant

The structural-model results presented in Table 4 indicated that all proposed direct and indirect relationships were positive and statistically significant. Strategic alignment and executive commitment had a strong positive effect on governance and policy development, with a standardized path coefficient of 0.58, a t value of 14.15, and a probability value below 0.001. The confidence interval ranged from 0.498 to 0.658 and did not include zero. The effect size for this relationship was 0.50, indicating a large contribution of strategic alignment and executive commitment to the development of organizational governance and formal policies. This finding demonstrated that organizations in which senior executives actively supported zero-trust transformation, allocated resources to the initiative, linked cybersecurity to organizational strategy, and established clear implementation priorities were substantially more likely to possess coherent governance structures, defined responsibilities, formal access-control policies, and coordinated decision-making processes.

Strategic alignment and executive commitment also had a significant positive effect on technological and infrastructural readiness, with a standardized coefficient of 0.37, a t value of 8.04, and a probability value below 0.001. The effect size was 0.16, representing a moderate effect. Therefore, senior-level strategic commitment appeared to facilitate investment in identity-management technologies, continuous authentication, network segmentation, device monitoring, data classification, security analytics, and modernization of legacy infrastructure. Strategic alignment and executive commitment also positively predicted human

resources and change management, with a standardized coefficient of 0.44, a t value of 10.00, and a probability value below 0.001. The effect size of 0.24 indicated a moderate-to-relatively-large contribution. This result suggested that executive commitment was associated not only with technical investment but also with employee education, specialized training, communication of implementation objectives, change leadership, participation of organizational units, and the management of resistance to new security procedures.

Governance and policy development had a significant positive effect on cybersecurity risk and compliance management, with a standardized coefficient of 0.49, a t value of 11.40, and a probability value below 0.001. The associated effect size was 0.32, indicating a relatively large effect. This finding showed that formal governance structures, role clarity, policy standardization, accountability, data governance, and coordination among organizational units substantially strengthened the organization's ability to identify cyber risks, maintain regulatory compliance, manage third-party access, respond to security incidents, and continuously evaluate changes in the threat environment.

Among the direct predictors of zero-trust implementation effectiveness, technological and infrastructural readiness had the strongest effect, with a standardized path coefficient of 0.30, a t value of 6.12, and a probability value below 0.001. Its effect size was 0.14, which represented a moderate practical contribution. This result indicated that the availability and integration of the required technological capabilities were central to effective zero-trust implementation. Organizations with more mature identity and access-management systems, stronger endpoint visibility, greater capacity for micro-segmentation, more comprehensive monitoring, and improved compatibility between security tools and legacy systems reported higher levels of threat detection, access control, incident containment, operational resilience, and protection of sensitive organizational information.

Governance and policy development exerted the second-largest direct managerial effect on zero-trust implementation effectiveness, with a standardized coefficient of 0.22, a t value of 4.23, and a probability value below 0.001. Its effect size was 0.07. This result suggested that technology alone was insufficient and that effective implementation depended on the formal definition of responsibilities, decision rights, access policies, data-ownership arrangements, accountability mechanisms, and cross-functional coordination. Cybersecurity risk and compliance management also had a significant positive effect on implementation effectiveness, with a standardized coefficient of 0.21, a t value of 4.20, and a probability value below 0.001. The effect size was 0.08. This relationship showed that organizations that systematically connected zero-trust practices to enterprise risk management, regulatory obligations, incident response, third-party risk, and continuous security assessment achieved more effective implementation outcomes.

Human resources and change management significantly predicted zero-trust implementation effectiveness, with a standardized coefficient of 0.19, a t value of 4.32, and a probability value below 0.001. The effect size of 0.08 indicated a meaningful contribution. Thus, employee awareness, technical competence, training quality, managerial communication, and the management of organizational resistance were associated with improved implementation results. This finding was especially important because the descriptive results showed that human resources and change management had the lowest mean score among the examined dimensions. The combination of a relatively low average score and a statistically significant structural effect indicated that human-resource readiness represented both an important determinant of effectiveness and a potential area of weakness in the participating organizations.

Strategic alignment and executive commitment retained a statistically significant direct effect on zero-trust implementation effectiveness after the mediating variables had been included in the model. The standardized direct coefficient was 0.14, with a t value of 2.98 and a probability value of 0.003. Although the direct effect size was relatively small, its statistical significance indicated that executive commitment contributed to implementation effectiveness beyond its effects through governance, infrastructure, and change management. Senior leadership may therefore influence implementation outcomes through additional mechanisms, including prioritization of the initiative, conflict resolution, resource protection, strategic continuity, interdepartmental authority, and the establishment of zero-trust implementation as an organization-wide responsibility rather than a narrowly technical project.

The analysis of indirect effects further clarified the mechanisms through which strategic-management capabilities influenced implementation effectiveness. The indirect effect of strategic alignment and executive commitment through governance and policy development

was 0.128 and was statistically significant at $p < 0.001$. Strategic alignment and executive commitment also had a significant indirect effect through technological and infrastructural readiness, with a coefficient of 0.111, and through human resources and change management, with a coefficient of 0.084. Because both the direct and indirect effects of strategic alignment and executive commitment were statistically significant, governance and policy development, technological readiness, and human resources and change management partially mediated the relationship between executive commitment and implementation effectiveness.

Governance and policy development also influenced implementation effectiveness indirectly through cybersecurity risk and compliance management. This indirect effect was 0.103, with a t value of 3.32 and a probability value of 0.001. Accordingly, formal governance arrangements increased implementation effectiveness both directly and by strengthening cybersecurity risk-management and compliance capabilities. The serial indirect pathway from strategic alignment and executive commitment through governance and policy development and subsequently through cybersecurity risk and compliance management was also significant, with a standardized coefficient of 0.060 and a probability value of 0.004. This serial relationship demonstrated that executive-level strategic commitment contributed to formal governance development, which subsequently enhanced risk and compliance management and ultimately improved zero-trust implementation effectiveness.

The total effect of strategic alignment and executive commitment on zero-trust implementation effectiveness was 0.523 when its direct and specific indirect effects were considered jointly. This finding identified strategic alignment and executive commitment as the most influential upstream strategic factor in the model, despite technological and infrastructural readiness having the strongest direct effect on implementation effectiveness. Similarly, the total effect of governance and policy development on implementation effectiveness was 0.323, consisting of its direct effect of 0.22 and its indirect effect of 0.103 through cybersecurity risk and compliance management. Therefore, the structural results showed that leadership and governance operated as enabling forces that shaped technical readiness, employee adaptation, risk management, and implementation performance.

The coefficient of determination for governance and policy development was 0.336, indicating that strategic alignment and executive commitment explained 33.6% of the variance in governance and policy development. The coefficient of determination for technological and infrastructural readiness was 0.137, meaning that executive commitment explained 13.7% of its variance. For human resources and change management, the coefficient of determination was 0.194, indicating that 19.4% of the variance was explained by strategic alignment and executive commitment. Governance and policy development explained 24.0% of the variance in cybersecurity risk and compliance management. Most importantly, the combined effects of strategic alignment and executive commitment, governance and policy development, technological and infrastructural readiness, human resources and change management, and cybersecurity risk and compliance management explained 68.3% of the variance in zero-trust implementation effectiveness. The adjusted coefficient of determination was 0.678, indicating that the model had substantial explanatory power and that the observed level of explained variance was not primarily attributable to the number of predictors.

The Stone–Geisser predictive-relevance value for zero-trust implementation effectiveness was 0.421, which was considerably greater than zero and demonstrated strong out-of-sample predictive relevance. The predictive-relevance values for governance and policy development, technological and infrastructural readiness, human resources and change management, and cybersecurity risk and compliance management were 0.198, 0.078, 0.116, and 0.145, respectively. All values were positive, indicating that the model had predictive relevance for each endogenous construct. Overall, the structural-model results supported the proposed relationships and demonstrated that effective zero-trust implementation in large organizations resulted from the coordinated interaction of executive leadership, formal governance, technological readiness, human-resource adaptation, and cybersecurity risk-management capabilities.

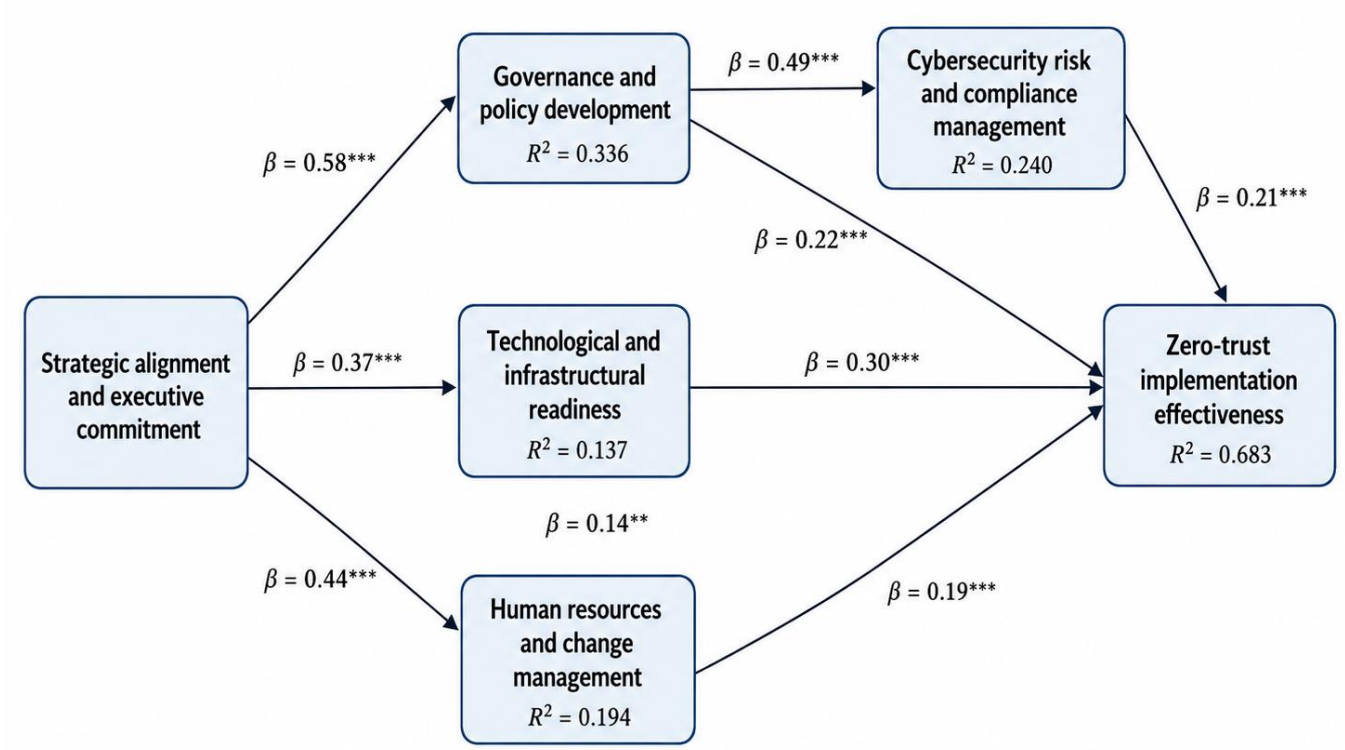

Figure 1. Final Structural Model of the Strategic Management Factors Affecting Zero-Trust Network Architecture Implementation Effectiveness

4. Discussion and Conclusion

The present study investigated the strategic, organizational, technological, and managerial determinants of effective zero-trust network architecture implementation in large organizations. The findings demonstrated that zero-trust implementation effectiveness was not attributable to a single technical capability; rather, it emerged from the coordinated interaction of strategic alignment and executive commitment, governance and policy development, technological and infrastructural readiness, human resources and change management, and cybersecurity risk and compliance management. The proposed model explained 68.3% of the variance in zero-trust implementation effectiveness, indicating substantial explanatory power. All direct and indirect paths were statistically significant, and the model possessed satisfactory predictive relevance. Among the direct predictors, technological and infrastructural readiness exerted the strongest effect on implementation effectiveness, followed by governance and policy development, cybersecurity risk and compliance management, human resources and change management, and strategic alignment and executive commitment. However, when direct and indirect effects were considered simultaneously, strategic alignment and executive commitment emerged as the most influential upstream factor. These results support the view that zero trust should be managed as an enterprise-wide strategic transformation rather than as a limited cybersecurity technology project.

The descriptive findings showed that strategic alignment and executive commitment received the highest mean score among the examined dimensions. This result suggests that the participating organizations generally recognized the strategic importance of zero trust and had achieved a relatively favorable level of senior-management support. Large organizations may increasingly perceive cyber risk as a business-continuity, governance, and reputational issue rather than solely as a technical concern. This interpretation is consistent with the broader evolution of zero trust from a network-security concept into an enterprise-security philosophy that connects access control, identity management, data protection, and organizational resilience [9, 12]. The finding also aligns with planning-oriented approaches emphasizing that successful zero-trust adoption requires executive sponsorship, phased implementation, resource prioritization, and integration with organizational objectives [5]. Nevertheless, the moderate rather than

exceptionally high mean indicates that strategic recognition may not yet have been fully translated into consistent organization-wide practices.

Human resources and change management obtained the lowest mean score. This result identifies employee readiness, organizational communication, specialized training, and resistance management as relatively underdeveloped aspects of zero-trust implementation. The finding is particularly important because zero trust alters routine work practices, authentication procedures, privilege structures, monitoring arrangements, and interactions with digital resources. Even technically advanced organizations may encounter implementation failure when users do not understand new security requirements or perceive controls as excessively restrictive. Reviews of zero-trust migration have similarly identified cultural resistance, insufficient skills, limited awareness, and organizational complexity as major implementation barriers [10, 22]. The comprehensive migration framework proposed by Phiayura and Teerakanok also emphasizes readiness assessment, phased transition, stakeholder involvement, and continuous adaptation rather than abrupt technological deployment [23]. Therefore, the relatively low human-resource score indicates that many organizations may have invested more rapidly in technical controls than in preparing personnel to adopt and sustain them.

The correlation results showed that all strategic-management dimensions were positively associated with zero-trust implementation effectiveness. Technological and infrastructural readiness displayed the strongest bivariate relationship with implementation effectiveness, followed by governance and policy development and cybersecurity risk and compliance management. These findings confirm that effective zero-trust implementation requires a foundation of identity-management capabilities, continuous authentication, device visibility, network segmentation, data classification, monitoring, and policy enforcement. This result is consistent with comparative reviews demonstrating that identity-centered access, micro-segmentation, endpoint security, contextual verification, and continuous monitoring are among the principal technical components of zero-trust models [6, 8]. Research on cloud networks likewise emphasizes the need to integrate identity, workload protection, policy enforcement, and continuous visibility across dynamic environments [15, 16]. The strength of the observed relationships therefore reflects the foundational role of technical readiness while also demonstrating that technical capability must operate alongside managerial and organizational mechanisms.

The structural analysis indicated that technological and infrastructural readiness had the strongest direct effect on zero-trust implementation effectiveness. This finding suggests that organizations cannot achieve the intended outcomes of zero trust without sufficiently mature security infrastructure. Strategic commitment and formal policy may provide direction, but their effects remain limited if the organization lacks interoperable authentication systems, endpoint visibility, segmentation capabilities, automated monitoring, and compatible legacy infrastructure. The result is aligned with research on Azure-based implementation, which shows that practical zero-trust adoption requires coordinated use of identity services, conditional access, security monitoring, device management, and cloud-protection capabilities [17]. It is also consistent with research on big-data platforms, where effective zero-trust design depends on adapting security controls to the architecture and sensitivity of organizational data resources [18]. Studies of secure enterprise networks further reinforce the importance of integrating access-control technologies across users, devices, applications, and distributed resources [3, 4].

Technological readiness may also explain why automation and intelligent security analytics are becoming increasingly important within zero-trust environments. Continuous verification generates a volume and velocity of security information that cannot be processed efficiently through manual procedures. Automated orchestration can facilitate real-time access adjustment, incident containment, policy enforcement, and coordinated response across multiple controls [19]. Similarly, machine-learning-based systems combining security information and event management, security orchestration and automated response, and user and entity behavior analytics can strengthen context-aware threat detection [20]. AI-supported zero-trust approaches may also help organizations evaluate complex or opaque digital systems, including cloud-hosted artificial intelligence services [21]. However, the current findings imply that these technologies produce meaningful implementation outcomes only when the underlying infrastructure is sufficiently integrated, scalable, and strategically governed.

Governance and policy development exerted a significant positive direct effect on zero-trust implementation effectiveness and also indirectly influenced effectiveness through cybersecurity risk and compliance management.

This result confirms that zero trust depends on formalized access rules, clear accountability, defined data ownership, coordinated decision rights, and consistent enforcement across organizational units. Without governance, different departments may configure incompatible policies, grant excessive exceptions, or interpret trust requirements inconsistently. The finding is compatible with research emphasizing the role of zero-trust access policies in protecting network infrastructure and users [13]. It is also aligned with the NIST model for cloud-native applications in multi-location environments, which highlights consistent access-control policy across distributed resources [14]. The indirect effect through risk and compliance management further demonstrates that governance improves implementation partly because it strengthens the organization's capacity to identify cyber risks, manage third-party access, maintain regulatory compliance, and respond to incidents.

Governance also had a strong positive effect on cybersecurity risk and compliance management. This finding can be explained by the fact that risk management requires clearly assigned responsibilities, standardized reporting, formal decision procedures, and mechanisms for monitoring compliance. When governance is fragmented, risk information may remain isolated within technical units and fail to influence organizational priorities. By contrast, coherent governance allows zero-trust controls to be prioritized according to asset criticality, threat exposure, operational consequences, and legal requirements. The result is consistent with the treatment of zero trust as a risk countermeasure whose value depends on organizational context, resource constraints, and the expected reduction of security exposure [26]. It also corresponds with work on advanced persistent threats, which suggests that continuous verification and restricted lateral movement can reduce the effectiveness of long-term intrusion strategies [27]. Therefore, governance serves as the bridge between technical controls and enterprise-level risk management.

Cybersecurity risk and compliance management had a significant direct effect on implementation effectiveness. This finding indicates that zero-trust initiatives are more effective when they are embedded in continuous risk assessment, incident response, regulatory compliance, third-party management, and data-protection processes. A technically sophisticated architecture may still perform poorly if controls are not aligned with actual threats and critical organizational assets. The banking-sector model proposed by Chaudhry and Hydros illustrates how zero-trust principles can be adapted to sector-specific requirements concerning data integrity, access, and transaction security [28]. Secure secret-management models for distributed financial applications likewise show that credentials, cryptographic keys, and service identities require explicit governance within zero-trust systems [29]. These studies support the present finding that zero-trust effectiveness depends on integrating architecture with risk-sensitive operational priorities.

Human resources and change management also significantly predicted implementation effectiveness. Although its path coefficient was smaller than that of technological readiness, its effect remained meaningful. This result indicates that employee awareness, professional expertise, communication, training, and resistance management contribute directly to the successful use of zero-trust controls. Continuous verification depends on user compliance with authentication procedures, secure handling of credentials, appropriate device use, and adherence to access policies. Furthermore, technical teams must possess the knowledge needed to integrate identity systems, monitor policy performance, and resolve conflicts between security and operational continuity. The challenge is especially pronounced in legacy industrial environments, where technical personnel must protect older systems without disrupting essential operations [24]. The evolution of cloud integration in operational-technology networks also demonstrates that personnel must manage increasingly complex relationships between traditional industrial systems and modern digital platforms [25]. Accordingly, human-resource development is not a peripheral support activity but a core implementation capability.

Strategic alignment and executive commitment had significant positive effects on governance and policy development, technological and infrastructural readiness, and human resources and change management. These results show that executive leadership functions as an upstream enabler of organizational readiness. Senior managers determine whether zero trust receives sustained funding, cross-functional authority, strategic priority, and organizational visibility. Their commitment also affects whether departments cooperate, whether legacy modernization is funded, and whether employee training is treated as an essential investment. The strong effect on governance is consistent with the argument that zero trust requires formal organizational authority rather than isolated technical experimentation. The effects on technology and human resources indicate that strategic commitment

translates into implementation through both infrastructure investment and change-management support. This interpretation is aligned with the view that zero trust is not a "magic bullet" but a complex transformation whose outcomes depend on realistic leadership and organizational preparation [11].

Although the direct effect of strategic alignment and executive commitment on implementation effectiveness was smaller than the other direct paths, its total effect was the largest because it operated through multiple mediators. Governance and policy development, technological and infrastructural readiness, and human resources and change management partially mediated the relationship between executive commitment and effectiveness. This finding provides an important theoretical contribution by demonstrating that leadership does not improve zero-trust outcomes primarily through symbolic support. Rather, executive commitment becomes effective when it is converted into formal governance, technical capability, and organizational preparedness. The significant serial indirect pathway through governance and cybersecurity risk management further showed that leadership influences implementation by shaping policies and accountability structures that subsequently strengthen risk-management practices. This result supports the progressive and multidimensional character of zero-trust migration described in previous literature [9, 23].

The explanatory power of the model demonstrates that zero-trust effectiveness is best understood through a socio-technical and strategic-management perspective. Technical architecture remains essential, but its effectiveness is conditioned by leadership, governance, personnel, and risk-management processes. This conclusion is consistent across diverse application environments. Decentralized zero-trust models require decisions concerning distributed authority and policy enforcement [32]; activity-control models require adaptive governance of user actions in collaborative systems [33]; and zero-trust approaches for unmanned aerial vehicles require policy adaptation to dynamic and resource-constrained environments [34]. Similarly, quantum-fingerprinting approaches for device access demonstrate that advanced verification mechanisms still need to be integrated within coherent security frameworks [35]. The application of zero trust to fifth-generation air interfaces and communication, navigation, and surveillance systems further illustrates that architecture must be adapted to mission requirements, availability needs, and domain-specific risks [30, 31]. Therefore, the present results extend the literature by empirically showing that diverse technical capabilities require coordinated strategic management to produce effective organizational outcomes.

This study had several limitations that should be considered when interpreting the findings. The cross-sectional design prevented definitive conclusions regarding causality or changes in implementation maturity over time. Data were collected through self-report questionnaires, which may have been influenced by social desirability, organizational optimism, or participants' incomplete knowledge of all aspects of zero-trust implementation. Although the sample included professionals from several sectors, all participating organizations were located in Tehran, which may limit the generalizability of the findings to organizations in other geographical, economic, or regulatory contexts. The study also examined implementation at an aggregate organizational level and did not independently verify technical configurations, security incidents, audit findings, or objective performance indicators. Moreover, the model focused on five major strategic-management dimensions and may not have captured other relevant factors, such as vendor dependence, organizational culture, budget constraints, supply-chain complexity, privacy concerns, or service-user experience.

Future studies should employ longitudinal designs to examine how strategic commitment, governance, technical readiness, and implementation effectiveness evolve across different stages of zero-trust adoption. Comparative research could investigate differences among public and private organizations, highly regulated and less regulated industries, and organizations with different levels of digital maturity. Mixed-method studies combining surveys with interviews, security audits, network-performance indicators, and incident data would provide a more comprehensive assessment of implementation effectiveness. Future researchers could also test additional mediating and moderating variables, including cybersecurity culture, organizational agility, perceived implementation complexity, budget adequacy, employee resistance, vendor support, and regulatory pressure. Multi-group structural analyses could determine whether the proposed relationships vary according to organization size, sector, ownership, cloud maturity, or prior experience with zero-trust technologies. Experimental or quasi-experimental evaluations of phased zero-trust interventions would also help identify which implementation practices produce the greatest improvement in measurable security and operational outcomes.

Large organizations should manage zero-trust implementation as a strategic transformation program with clear executive ownership, measurable objectives, and cross-functional governance. Senior managers should establish a steering structure involving cybersecurity, information technology, risk management, legal, human resources, internal audit, and business-unit representatives. Implementation should begin with the identification of critical assets, privileged identities, sensitive data, and high-risk access pathways, followed by phased deployment of identity management, multifactor authentication, device assessment, segmentation, monitoring, and automated policy enforcement. Organizations should avoid treating technology acquisition as sufficient and should invest equally in employee education, specialist training, communication, and resistance management. Policies should be reviewed continuously and linked to enterprise risk assessments, regulatory obligations, incident-response procedures, and third-party access requirements. Finally, organizations should define performance indicators for access violations, lateral movement, authentication failures, policy exceptions, incident-containment time, user disruption, and operational resilience so that zero-trust effectiveness can be evaluated and improved over time.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] A. Wylde, "Zero Trust: Never Trust, Always Verify," pp. 1-4, 2021, doi: 10.1109/cybersa52016.2021.9478244.

[2] C. Sample, C. Shelton, S. M. Loo, C. Justice, L. Hornung, and I. Poynter, "ZTA: Never Trust, Always Verify," *European Conference on Cyber Warfare and Security,* vol. 21, no. 1, pp. 256-262, 2022, doi: 10.34190/eccws.21.1.309.

[3] R. Chandramouli, "Guide to Secure Enterprise Network Access Landscape," 2022, doi: 10.6028/nist.sp.800-215.ipd.

[4] R. Chandramouli, "Guide to a Secure Enterprise Network Landscape," 2022, doi: 10.6028/nist.sp.800-215.

[5] S. Rose, "Planning for a Zero Trust Architecture," 2022, doi: 10.6028/nist.cswp.20.

[6] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing,* vol. 2022, no. 1, 2022, doi: 10.1155/2022/6476274.

[7] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," *Entropy,* vol. 25, no. 12, p. 1595, 2023, doi: 10.3390/e25121595.

[8] P. Dhiman *et al.*, "A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model," *Sensors,* vol. 24, no. 4, p. 1328, 2024, doi: 10.3390/s24041328.

[9] S. K. Nanda and R. Priyadarshini, "A Comprehensive Review and Comparative Analysis of Zero Trust Architecture: Evolution, Implementation Strategies, and Key Challenges," *Journal of Computer Security,* vol. 34, no. 2, pp. 85-110, 2025, doi: 10.1177/0926227x251409922.

[10] S. Mushtaq, M. Mohsin, and M. Mushtaq, "A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains," *Sensors,* vol. 25, no. 19, p. 6118, 2025, doi: 10.3390/s25196118.

[11] H. Salminen, "Zero Trust: The Magic Bullet or Devil's Advocate?," *European Conference on Cyber Warfare and Security,* vol. 22, no. 1, pp. 678-686, 2023, doi: 10.34190/eccws.22.1.1263.

[12] K. M. Adamson and A. Qureshi, "Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA," 2025, doi: 10.21203/rs.3.rs-6602547/v1.

[13] I. Ogbaga, C. Ogbonnaya, and A. Chukwuemeka, "Deployment of Zero Trust Access (ZTA) Policy as a Veritable Tool for Protecting Network Infrastructures and Users," 2023, doi: 10.20944/preprints202307.0006.v1.

[14] R. Chandramouli and Z. Butcher, "A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments," 2023, doi: 10.6028/nist.sp.800-207a.

[15] S. Sarkar, G. Choudhary, S. K. Shandilya, H. Azath, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustainability,* vol. 14, no. 18, p. 11213, 2022, doi: 10.3390/su141811213.

[16] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," 2024, doi: 10.31219/osf.io/dt4km.

[17] V. Dakić, Z. Morić, A. Kapulica, and D. Regvart, "Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations," 2024, doi: 10.20944/preprints202407.1454.v1.

[18] R. Li and X. Cao, "Research on the Design of Network Security System for Natural Resources Big Data Platform Based on Zero-Trust Architecture," p. 81, 2024, doi: 10.1117/12.3038292.

[19] Y. Cao, S. R. Pokhrel, Y. Zhu, R. Doss, and G. Li, "Automation and Orchestration of Zero Trust Architecture:Potential Solutions and Challenges," 2022, doi: 10.36227/techrxiv.21385929.

[20] A. Hassan, A. Rauf, N. Shafqat, R. Latif, and H. Khan, "ZenGuard a Machine Learning Based Zero Trust Framework for Context Aware Threat Mitigation Using SIEM SOAR and

UEBA," *Scientific Reports,* vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-20998-4.
[21] B. Dash, "Zero-Trust Architecture (ZTA): Designing an AI-Powered Cloud Security Framework for LLMs' Black Box Problems," *Current Trends in Eng Sc,* vol. 4, no. 2, pp. 1-5, 2024, doi: 10.54026/ctes/1058.
[22] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges," *Security and Communication Networks,* vol. 2021, pp. 1-10, 2021, doi: 10.1155/2021/9947347.
[23] P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *Ieee Access,* vol. 11, pp. 19487-19511, 2023, doi: 10.1109/access.2023.3248622.
[24] A. Akinsanya, "Manufacturing Cybersecurity for SMEs: Implementing Zero Trust in Legacy Industrial Environments," 2026, doi: 10.21203/rs.3.rs-8846670/v1.
[25] C. Perducat, D. C. Mazur, W. Mukai, S. N. Sandler, M. Anthony, and J. Mills, "Evolution and Trends of Cloud on Industrial OT Networks," *Ieee Open Journal of Industry Applications,* vol. 4, pp. 291-303, 2023, doi: 10.1109/ojia.2023.3309669.
[26] A. M. Abdelmagid and R. Díaz, "Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems," *Risk Analysis,* vol. 45, no. 8, pp. 2390-2414, 2025, doi: 10.1111/risa.70026.
[27] B. Karabacak and T. N. Whittaker, "Zero Trust and Advanced Persistent Threats: Who Will Win the War?," *International Conference on Cyber Warfare and Security,* vol. 17, no. 1, pp. 92-101, 2022, doi: 10.34190/iccws.17.1.10.
[28] U. B. Chaudhry and A. K. M. Hydros, "Zero-trust-based Security Model Against Data Breaches in the Banking Sector: A Blockchain Consensus Algorithm," *Iet Blockchain,* vol. 3, no. 2, pp. 98-115, 2023, doi: 10.1049/blc2.12028.
[29] A. Siddiki, "Vault-Based Secret Management and Zero-Trust Security Model for Distributed Financial Applications," 2026, doi: 10.21203/rs.3.rs-9916782/v1.
[30] S. Sun, M. Repeta, V. Nandall, E. Fung, and C. D. Thomas, "Towards 5G Zero Trusted Air Interface Architecture," 2022, doi: 10.48550/arxiv.2211.03776.
[31] N. Ngema, B. Nleya, and R. C. Maswanganyi, "A Review of Zero Trust Architecture: Principles, Applications, and Implementation Challenges in Communication, Navigation, and Surveillance (CNS) Systems," *Sensors,* vol. 26, no. 12, p. 3813, 2026, doi: 10.3390/s26123813.
[32] S. R. Pokhrel, G. Li, R. Doss, and S. Nepal, "Towards Decentralized Operationalization of Zero Trust Architecture," 2022, doi: 10.36227/techrxiv.19127090.
[33] T. Mawla, M. Gupta, and R. Sandhu, "BlueSky: Activity Control: A Vision for "Active" Security Models for Smart Collaborative Systems," pp. 207-216, 2022, doi: 10.1145/3532105.3535017.
[34] A. Alquwayzani and A. Albuali, "A Systematic Literature Review of Zero Trust Architecture for UAV Security Systems in IoBT," 2024, doi: 10.20944/preprints202403.0349.v1.
[35] Z. Bassfar, A. Sayeed, P. H. M. Bala, A. Alshehri, A. M. Alanazi, and S. Zubair, "Toward Secure and Resilient Networks: A Zero-Trust Security Framework With Quantum Fingerprinting for Devices Accessing Network," *Mathematics,* vol. 11, no. 12, p. 2653, 2023, doi: 10.3390/math11122653.
[36] S. Yevseiev *et al.*, "The Concept of Building Security of the Network With Elements of the Semiotic Approach," *Sciencerise,* no. 1, pp. 24-34, 2023, doi: 10.21303/2313-8416.2023.002828.