Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Zero Trust for IT Governance and Risk Management: A Systematic Review and Conceptual Framework

nabil almotawkel

dr.almotawkel@21umas.edu.ye

21 September University for Medical and Applied Sciences https://orcid.org/0009-0009-0086-5905

Mohammed Alkohali

Emirates International University

Sadeg Manaa

International University of Technology Twintech

Osamah AL-Maamari

Al-Razi University

Ashraf Al-Godami

Sana'a University

Shaima Alqahoom

Dr. Babasaheb Ambedkar Marathwada University

Systematic Review

Keywords: Zero Trust Architecture, Cyber Risk Management, IT Governance, Systematic Literature Review (SLR), Artificial Intelligence, Blockchain, Critical Infrastructure, Organizational Culture

Posted Date: July 21st, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10392666/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Zero Trust for IT Governance and Risk Management: A Systematic Review and Conceptual Framework

Nabil Abdallh Abbas Almotawkel

21 September University for Medical and Applied Sciences, Faculty of Engineering and Computer Sciences, Sana'a, Yemen

dr.almotawkel@21umas.edu.ye

Mohammed Abdullah Sarhan Alkohali

Emirates International University, College of Management, Sana'a, Yemen

dr.m.alkohali@eiu.edu.ye

Sadeg Ali Yahyaa Manaa

International University of Technology Twintech, Sana'a, Yemen

Dr.sadekmanaa77@iutt.edu.ye

Osamah Ahmed AL-Maamari

Al-Razi University, Department of International Business Administration, Sanaa, Yemen

o.almaamari@alraziuni.edu.ye

Ashraf Yahia Hussein Al-Godami

Sana'a University, College of Management, Sana'a, Yemen

ashrafalgodami@su.edu.ys

Shaima Ameen Mansoor Alqahoom

Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar - 431004, Maharashtra, India

commerce.sam@bamu.ac.in

Abstract

The erosion of traditional network perimeters has challenged conventional security models, prompting growing interest in Zero Trust (ZT) architectures. While much of the existing literature focuses on technical implementations, there remains a significant gap in understanding the organizational and governance implications of ZT adoption. This study addresses this gap by synthesizing the fragmented cybersecurity governance literature using a rigorous, evidence-based review protocol (PRISMA 2020) to examine how Zero Trust impacts risk management and IT governance in organizational information systems, including emerging digital government contexts. A structured search across Scopus, Google Scholar, and Dimensions (2020–2026) yielded 73 peer-reviewed studies for final synthesis. The analysis integrates thematic synthesis and bibliometric mapping to identify key mechanisms—including continuous verification, micro-segmentation, and identity-centric access—and their translation into governance outcomes. Findings indicate that Zero Trust enhances threat visibility, limits lateral movement, and supports compliance alignment, although its effectiveness varies considerably with organizational culture, regulatory maturity, and implementation context. The study proposes an integrative framework linking technical controls to strategic governance objectives. This review contributes

evidence-based insights for practitioners and policymakers, while identifying critical research gaps in SME adoption, AI-driven automation, and longitudinal maturity models.

Keywords

Zero Trust Architecture; Cyber Risk Management; IT Governance; Systematic Literature Review (SLR); Artificial Intelligence; Blockchain; Critical Infrastructure; Organizational Culture.

1. Introduction

The accelerating convergence of digital technologies—spanning cloud computing, the Internet of Things (IoT), artificial intelligence (AI), and next-generation communication infrastructures—has substantially reconfigured into distributed and highly dynamic socio-technical ecosystems. While this transformation has enabled significant levels, it has simultaneously destabilized the foundational assumptions underpinning traditional cybersecurity and governance models. In particular, the erosion of clearly defined network perimeters and the proliferation of identity-centric access have rendered perimeter-based security architectures increasingly ineffective, exposing organizations to advanced threats characterized by lateral movement, credential compromise, and persistent insider risks [1]; [2]. This structural disjunction has catalyzed a broader epistemic shift in how risk, trust, and governance are conceptualized within digital environments. Within this evolving landscape, Zero Trust (ZT) has emerged not merely as a technical architecture but as a major reconfiguration. By rejecting implicit trust and enforcing continuous, context-aware verification, ZT reframes security as a dynamic and adaptive process grounded in identity, behaviour, and situational awareness [3]; [4]. Importantly, its implications extend beyond technical controls to intersect with enterprise risk management and IT governance, repositioning trust as a continuously negotiated condition rather than a static organizational asset [5]; [6]. Despite its rapid diffusion, the literature on Zero Trust remains fragmented and conceptually inconsistent. A dominant stream focuses on technical mechanisms such as micro-segmentation and access control [7]; [8], whereas an emerging body of research conceptualizes ZT as a governance paradigm influencing compliance, accountability, and decision-making [9]; [1]. This divergence reflects deeper theoretical tensions regarding the locus of cybersecurity—whether as infrastructure or governance—resulting in parallel yet insufficiently integrated research trajectories. Moreover, much of the existing work is either context-specific or normatively oriented, limiting its generalizability and empirical robustness [10]; [3]. A critical limitation of current scholarship lies in the disconnect between technical security capabilities and governance outcomes. While ZT is widely associated with improved visibility and threat mitigation, its translation into organizational-level benefits—such as compliance, auditability, and strategic alignment—remains underexplored [11]; [12]. This gap is particularly problematic in the context of enterprise risk management, where cybersecurity is increasingly expected to integrate with broader governance frameworks. Furthermore, empirical findings indicate that the effectiveness of ZT depends considerably on contextual factors, including organizational culture, maturity, and regulatory environment [3]; [13]. These contingencies challenge universalist assumptions and highlight the need for a multi-level analytical perspective. The complexity of this landscape is further intensified by the integration of emerging technologies such as AI, which simultaneously enhances and destabilizes cybersecurity practices. While AI enables predictive risk assessment and automated response, it also introduces novel vulnerabilities and epistemic uncertainties [14]; [15]. Consequently, traditional risk management frameworks—often static and compliance-driven—are increasingly misaligned with the dynamic and adversarial nature of contemporary digital ecosystems [11]. Despite the growing volume of research, the field lacks a coherent synthesis capable of integrating these diverse perspectives. Existing reviews tend to isolate either technical or sectoral dimensions, failing to capture the multidimensional impact of Zero Trust across risk management and governance domains. This gap is particularly evident in light of the substantial body of peer-reviewed studies systematically identified and curated within this research, which reflects both the maturity and fragmentation of the field. In response, this study advances a systematic review that conceptualizes Zero Trust as a socio-technical paradigm operating across interconnected layers of security mechanisms, risk management processes, and governance outcomes. Through a rigorous synthesis of the literature, the analysis implicitly examines how ZT reshapes risk identification, mitigation, and response, and how these transformations translate into governance effectiveness within organizational information systems. By adopting a comparative logic that contrasts ZT with traditional models, the study provides a more nuanced evaluation of its transformative potential. Methodologically, a systematic review integrating thematic synthesis is employed as a suitable epistemological approach to reconcile fragmentation and heterogeneity within the literature. This strategy enables the identification of patterns of convergence

and divergence while preserving contextual nuance across studies. Preliminary synthesis reveals consistent agreement on the role of ZT in enhancing system visibility and adaptive risk management [16]; [17], alongside divergence regarding implementation complexity and organizational readiness [4]; [3]. These findings underscore the need for an integrative framework capable of capturing the conditional and mediated nature of ZT impacts. Theoretically, this study contributes by bridging cybersecurity and IT governance through an integrative framework grounded in enterprise risk management and informed by Principal–Agent Theory, reframing trust as a continuously verifiable construct [9]. Practically, it offers evidence-based insights to guide organizations and policymakers in aligning Zero Trust implementation with governance objectives and regulatory requirements. In sum, this article provides a theoretically grounded and empirically informed synthesis of the impact of Zero Trust on risk management and IT governance, addressing a critical gap in the literature and advancing both scholarly understanding and practical application. While existing studies have examined Zero Trust from a purely engineering perspective, this review addresses a critical gap in the managerial and governance literature. By synthesizing fragmented evidence, our framework provides Chief Information Security Officers (CISOs), risk managers, and IT auditors with a clear roadmap to align cybersecurity investments with strategic business objectives and regulatory mandates such as GDPR and NIS 2. Rather than treating Zero Trust merely as a technical upgrade, we conceptualize it as a socio-technical governance paradigm that requires alignment between continuous verification, organizational culture, and regulatory frameworks. The remainder of the paper proceeds with the methodological framework, followed by the presentation of findings, a theory-driven discussion, and concluding insights.

2. Methodology

2.1 Research Design

This study adopts a hybrid methodological design integrating a systematic literature review (SLR), bibliometric analysis, and conceptual framework development to examine the impact of Zero Trust on risk management and IT governance. This design is particularly suited to interdisciplinary domains where cybersecurity architectures intersect with organizational governance and enterprise risk management [9]. The hybrid approach directly addresses documented limitations of traditional perimeter-based models [5] while accounting for the recognized influence of organizational culture and contextual factors on cybersecurity adoption [3]. To ensure transparency and replicability, the SLR adheres to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol [18]; [19]. This framework operationalizes a standardized four-stage process—identification, screening, eligibility, and inclusion—designed to minimize selection bias. The search strategy targets key academic databases (Scopus, IEEE Xplore, Web of Science, ScienceDirect, and the ACM Digital Library) to capture both technical security architectures and managerial perspectives [18]. For data interpretation, thematic synthesis is employed using qualitative analysis software (ATLAS.ti) to systematically identify core constructs—including interdependency, attack surface, and organizational risk behaviors—transforming unstructured qualitative data into structured conceptual knowledge [6]; [20]. To map the intellectual landscape, bibliometric analysis (via VOSviewer) is conducted to identify thematic clusters, historical trends, and evolving knowledge structures across critical sectors (e.g., maritime, energy, and finance) [20]; [21]. The conceptual framework is developed following Design Science Research (DSR) principles, serving as a "knowledge artifact" that bridges technical security controls and strategic IT governance requirements [20]. It incorporates established international standards—ISO 31000, ISO 27005, and the NIST Cybersecurity Framework— It incorporates established international standards—ISO 31000, ISO 27005, and the NIST Cybersecurity Framework to ensure practical applicability within professional risk management contexts [22]. This integrated approach facilitates the dual assessment of process maturity and control effectiveness, providing a robust tool for decision-makers navigating digital transformation. The detailed operationalization of the PICO framework and eligibility criteria are provided in Supplementary Materials A (Table S1) and Supplementary Materials B (Table S4).

2.2 Search Strategy and Study Selection

The review followed a structured protocol developed a priori to ensure consistency, transparency, and methodological rigor. The study protocol was prospectively registered on the Open Science Framework (OSF) prior to study execution to enhance transparency and reproducibility. The research question was structured using the PICO/PECO framework to define the population, intervention/exposure, comparison,

and outcomes relevant to Zero Trust Architecture and risk management research. The detailed framework is provided in Supplementary Materials A (Table S1: Operationalization of the PICO/PECO Framework for Zero Trust Architecture and Risk Management, 2017–2026).

Table 1: Operationalization of the PICO/PECO Framework

Element	Description
P (Population)	Organizational information systems and IT governance
I (Intervention)	Implementation of Zero Trust frameworks
C (Comparison)	Traditional security models
O (Outcome)	Impact on risk management, threat mitigation, compliance, and governance effectiveness

To enhance methodological transparency and ensure alignment between the research question, eligibility criteria, data extraction, and thematic synthesis, the PICO framework was further operationalized across the reviewed literature. This operationalization specified the population, intervention, comparison, and outcome dimensions in relation to Zero Trust implementation and risk management contexts. The detailed framework is provided in Supplementary Materials A Table S1 Operationalization of the PICO/PECO Framework for Zero Trust Architecture and Risk Management (2020–2026). The use of PICO is justified because Zero Trust represents a strategic intervention influencing both technical and organizational dimensions of risk management [3].
The central research question is:

What is the impact of implementing Zero Trust frameworks on risk management outcomes in organizational information systems and IT governance?

A comprehensive and reproducible search strategy was conducted using Google Scholar (via Harzing's Publish or Perish), Scopus, and Dimensions. A structured Boolean framework was developed based on key conceptual dimensions, including Zero Trust technologies, risk management, information systems, and governance outcomes. The full search strings and keyword mapping are detailed in Supplementary Materials B. The full Boolean search strategy is provided in Supplementary Materials B (Table S2: Core Boolean Search Strategy), while the extended thematic keyword mapping and domain-specific search strings are detailed in Supplementary Materials B (Table S3: Keywords and Boolean Search Strings). The search covered peer-reviewed publications from 1 January 2020 to 31 March 2026, ensuring inclusion of foundational and recent literature. In Google Scholar, the query "zero trust" AND "risk management" AND ("information system" OR "IT governance") AND ("impact" OR "implication") was applied as a simplified version of the full Boolean strategy. This reflected the broader multi-dimensional search design. Results show a clear growth trajectory in the field, increasing from limited publications in 2020 to 626 publications by Q1 2026. Initial retrieval yielded 1,695 records from Google Scholar, 305 from Scopus after filtering (year, subject area, document type, and keywords), and 6 from Dimensions. All records were managed using Zotero, producing a consolidated dataset of 2,006 studies, which was subsequently refined through screening to a final sample of 73 studies.

A multi-stage screening process was implemented to ensure methodological rigor, transparency, and reproducibility. Predefined inclusion and exclusion criteria—covering relevance, methodological quality, study design, data reporting, and source reliability—were systematically applied and are detailed in Supplementary Materials B (Table S4). Initially, 760 records were removed, including 87 duplicates (via Zotero and Rayyan) and 673 non-eligible sources such as non-academic publications, advertisements, company reports, white papers, news articles, blogs, and web-based materials due to lack of peer review and methodological rigor. Books and conference papers were also excluded to maintain focus on peer-reviewed journal articles. After pre-screening, 1,246 records remained for title and abstract screening, of which 908 were excluded for lack of relevance. A total of 338 full-text articles were assessed, but 129 were inaccessible. From the remaining 209 studies, 156 were excluded due to publication in non-impact factor journals (n = 97) and insufficient methodological quality or unclear relevance (n = 59). Additionally, 36 records were identified through citation tracking (Research Rabbit), of which 22 were retained after screening and full-text assessment. The study selection process is documented in the PRISMA 2020 flow diagram (Figure 1). The final dataset comprised 73 studies.

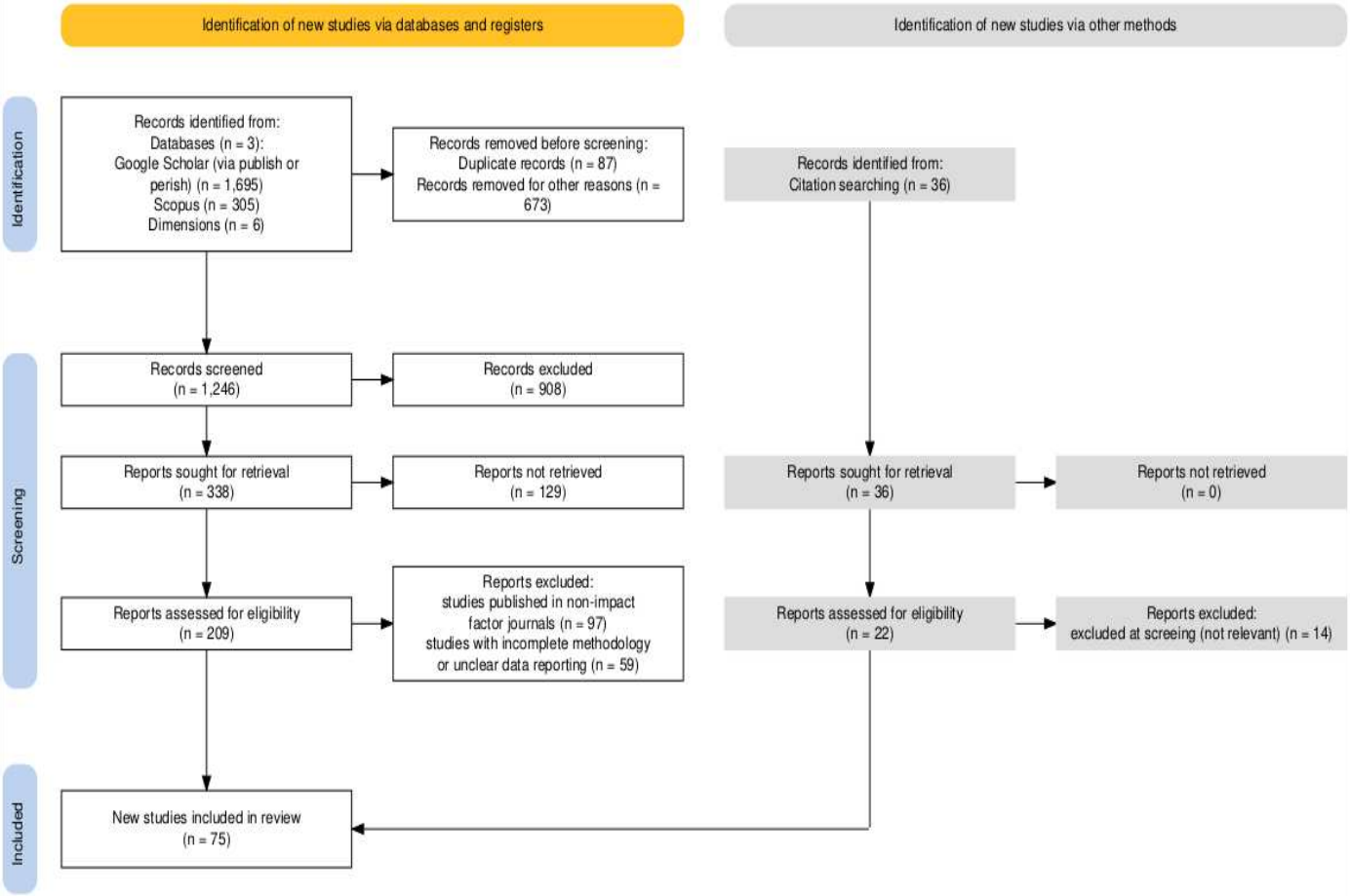


Figure 1. PRISMA flow diagram of the study selection process

2.3 Quality Appraisal and Data Extraction

This review combined structured appraisal criteria with expert judgment to ensure methodological rigor and conceptual relevance. Each study was independently evaluated by at least two reviewers using a CASP-based framework, with disagreements resolved through discussion or a third reviewer. Inter-rater reliability was assessed using Cohen's Kappa, confirming strong agreement. Expert rankings were considered consistent when consistency ratios remained within acceptable thresholds [23]; [24]. To ensure full transparency and reproducibility, the detailed screening workflow, reviewer assignment matrix, and Kappa calculation procedures are provided in the Supplementary Materials (Table S5: Study Screening Sheet, Table S6: Reviewer Assignment Matrix, and Table S7: Kappa Calculation Sheet). Full transparency is further ensured through Supplementary Materials, including the screening workflow, reviewer assignment matrix, and Kappa calculations (Tables S5–S7). A complete bibliographic overview of all included studies (N = 73) is provided in Supplementary Table S8. Given the heterogeneity of cybersecurity studies, a modified CASP framework was applied across analytical, observational, conceptual, and review-based designs. This adaptation was necessary due to the early-stage nature of Zero Trust research and its limited empirical maturity [25].

Conceptual studies

were excluded from formal risk-of-bias assessment, while additional criteria—relevance, reporting clarity, and conceptual contribution—were incorporated to reflect ZTA as a socio-technical and governance-oriented paradigm [4]. CASP criteria are detailed in Supplementary Table S11. To reduce publication bias and improve coverage, backward and forward snowballing was applied, supported by a longitudinal perspective to capture evolving trends [26]. This yielded 36 additional records; 14 were excluded, and 22 were assessed

for full-text eligibility. All retrieved records were successfully obtained. Studies were classified as strict (15), high-quality (28), moderate (7), and limited (25), as summarized in Supplementary Table S10. A detailed CASP-based appraisal with item-level judgments is provided in Supplementary Table S9, while a structured scoring-based assessment is presented in Supplementary Table S12. This multi-layered approach ensures methodological consistency and reproducibility across the dataset [23]. Overall, the final dataset included 73 studies, integrating analytical depth and contextual breadth through risk-informed, criteria-based selection aligned with research objectives [4].

2.4 Bibliometric and Topic Modeling Analysis

Bibliometric analysis was conducted to map the structure and evolution of the research field, with particular emphasis on the role of Zero Trust in cybersecurity. Bibliometric analysis was conducted using VOSviewer to map the intellectual structure of the field through keyword co-occurrence analysis, identifying thematic clusters, inter-topic relationships, and structural patterns within the research domain. The dataset was cleaned and standardized using Zotero to ensure consistency in author names, affiliations, and keywords. To complement this structural mapping, Latent Dirichlet Allocation (LDA) was applied to titles and abstracts using Python (Gensim) to uncover latent semantic themes, with the optimal number of topics determined via coherence score optimization. Text preprocessing included tokenization, stopword removal, and lemmatization to enhance interpretability. The integration of bibliometric analysis (structural relationships) and LDA (latent semantic content) enables triangulation, improving the validity and depth of findings [16].

2.5 Framework Development and Synthesis

The conceptual framework was developed through synthesis of systematic review findings and bibliometric insights. Zero Trust is conceptualized as a risk management paradigm emphasizing continuous verification and elimination of implicit trust [4]. These principles enable organizations to adopt proactive and adaptive security strategies.

The framework identifies:

- antecedents (cyber threats, digital transformation)
- mechanisms (authentication, monitoring)
- outcomes (risk reduction, governance effectiveness)

This structure reflects the role of Zero Trust in enhancing organizational resilience.

The study employed a narrative synthesis approach integrating systematic review findings with bibliometric analysis. Zero Trust contributes to improved risk management by reducing vulnerabilities and strengthening governance structures [5]; [13]. Methodological rigor was ensured through:

- structured protocol
- multi-stage filtering
- transparent criteria
- integration of multiple methods

However, limitations include database bias and reliance on indexed literature.

3. Results

3.1 Study Selection and Characteristics of Included Studies

The systematic identification process yielded 2,006 records following integration across multiple academic databases, reflecting a broad and heterogeneous evidence base aligned with the predefined search strategy [27]; [28]. After removing 760 records—including duplicates and ineligible studies—1,246 records were screened, leading to the exclusion of 908 studies due to limited relevance [29]. Of the remaining studies, 209

full-text articles were assessed for eligibility, with 156 excluded based on predefined criteria. Additional citation searching contributed further records, resulting in a final synthesis of 73 studies in accordance with PRISMA guidelines [30]; [31]. The included studies (N = 73) exhibit substantial diversity across temporal, geographic, methodological, and technological dimensions, reflecting the interdisciplinary nature of Zero Trust research. A pronounced concentration of studies is observed in recent years, particularly between 2023 and 2025, indicating an accelerated research trajectory aligned with increasing cybersecurity threats and digital transformation initiatives [14]; [9]. Bibliometric trends further confirm sustained growth in research output since 2018 [29]. Geographically, research activity is concentrated in Europe (26.7%), Asia-Pacific (21.3%), and the Middle East and North Africa (18.7%), while North America contributes 13.3% and Africa remains underrepresented [12]; [32]. This transformation is particularly pertinent for public sector organizations undergoing digital government modernization, where Zero Trust principles offer a pathway to secure citizen-centric services [1]; [8]. From a technological perspective, Zero Trust Architecture (ZTA) emerges as the dominant paradigm, supported by identity and access management, network security and micro-segmentation, cloud security, and AI-driven mechanisms, reinforcing its role as an integrated socio-technical ecosystem rather than a standalone solution. Furthermore, this upward trend in research activity aligns with a significant shift in threat actor motivations, moving away from simple digital vandalism toward sophisticated, financially motivated operations and strategic disruptions targeting high-value assets [26]. The integration of emerging technologies—such as 5G/6G networks and the Internet of Things (IoT)—has considerably expanded the attack surface, particularly for autonomous systems and smart city infrastructures, making Zero Trust an increasingly important architectural requirement rather than an optional enhancement [33]; [34]. In critical sectors like energy and railway transportation, the transition to this paradigm is frequently complicated by the presence of legacy systems, necessitating a phased, risk-based approach to de-perimeterization that balances operational continuity with enhanced data protection [4]; [23]. Ultimately, this systematic synthesis underscores Zero Trust's evolution into a foundational framework for cyber resilience, shifting organizations from a reactive defense posture to an anticipatory, data-driven security model capable of mitigating complex socio-technical risks [35]; [25].

Geographic Distribution

Geographically, research is concentrated in technologically advanced and regulation-intensive regions, with Europe leading, followed by Asia-Pacific and the MENA region. North America contributes a moderate share, while Latin America and Africa remain underrepresented.

Table 2. Temporal Distribution of Included Studies (N = 73)

Year	Number of Studies	Percentage (%)
2021	4	6.7%
2022	7	12.0%
2023	22	33.3%
2024	20	24.0%
2025	16	20.0%
2026	4	4.0%
Total	73	100%

The temporal distribution shows a sharp increase in publications between 2023 and 2025, indicating a rapid transition of Zero Trust from a conceptual model to a widely studied research domain, driven by growing recognition of its importance in addressing evolving cybersecurity risks.

Table 3. Core Studies

Year	Core Studies	Percentage (%)
2021	3	7.5%
2022	6	15.0%
2023	14	35.0%
2024	9	22.5%
2025	6	15.0%

Year	Core Studies	Percentage (%)
2026	2	5.0%
Total	40	100%

While the overall distribution shows a peak in 2023, the core studies confirm that this trend is not driven by peripheral research but reflects a genuine increase in Zero Trust-focused investigations.

Table 4. Geographic Distribution of Included Studies (N = 73)

Region / Country Cluster	Frequency	Percentage (%)	Analytical Insight
Europe	19	26.7%	Strong focus on governance, compliance, and regulatory frameworks (e.g., GDPR)
Asia-Pacific	16	21.3%	Emphasis on emerging technologies (AI, 5G, IoT)
Middle East & North Africa (MENA)	13	18.7%	Rapid adoption in public sector and smart infrastructure
North America	10	13.3%	Conceptual leadership and enterprise security models
Global / Multi-region	8	10.7%	Cross-sectoral and SME-oriented research
Latin America	6	8.0%	Emerging contributions linked to digital transformation
Africa	1	1.3%	Limited but growing research presence
Total	73	100%	

This distribution highlights the influence of regulatory maturity and digital transformation on Zero Trust adoption. European studies tend to prioritize governance and compliance, while Asia-Pacific research emphasizes technological innovation. In contrast, MENA studies reflect increasing strategic adoption in public sector transformation initiatives.

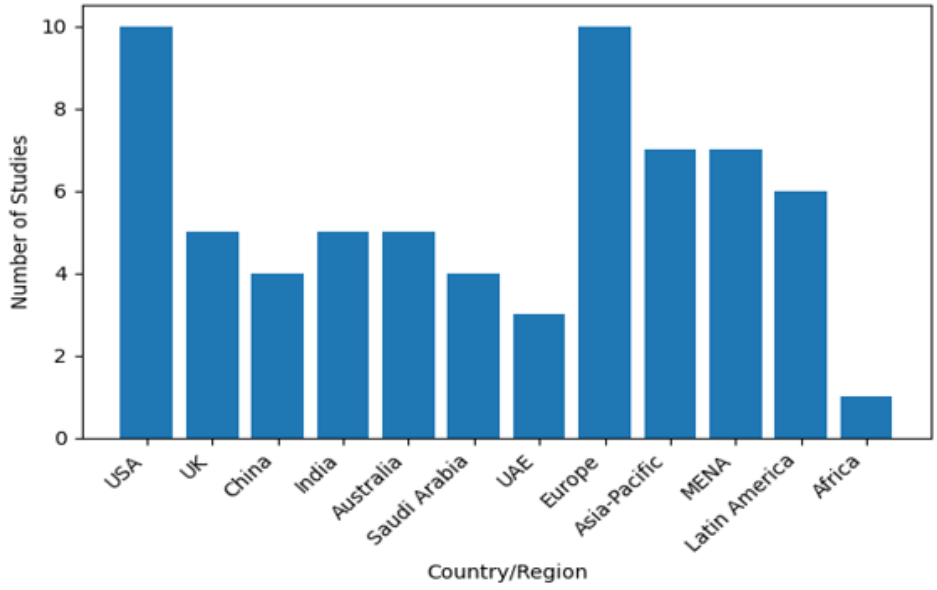


Figure 2. Global Distribution of Studies

Methodological Approaches

The methodological landscape of the reviewed studies is diverse, reflecting the complexity of Zero Trust as a socio-technical paradigm. Conceptual and theoretical studies dominate, indicating that the field is still undergoing theoretical consolidation. Empirical approaches—both quantitative and qualitative—complement this by providing context-specific insights into implementation and governance challenges.

Table 5. Methodological Approaches of Included Studies (N = 73)

Methodological Approach	Frequency	Percentage (%)	Analytical Insight
Conceptual / Theoretical	21	29.3%	Indicates ongoing theoretical development of Zero Trust
Empirical Quantitative	14	20.0%	Focus on statistical validation and risk modelling
Empirical Qualitative	12	16.0%	Explores organizational and governance dynamics
Case Studies	10	13.3%	Sector-specific insights (government, SMEs, healthcare)
Mixed Methods	9	12.0%	Integration of technical and organizational perspectives
Systematic Reviews / Surveys	7	9.3%	Consolidation and synthesis of existing knowledge
Total	73	100%	

This methodological diversity highlights the need to integrate technical, organizational, and governance perspectives in Zero Trust research. While conceptual studies drive ongoing theoretical development, empirical work increasingly validates implementation outcomes.

Primary Technology Focus

The studies consistently identify Zero Trust Architecture (ZTA) as the dominant paradigm, supported by complementary technologies enabling deployment in complex distributed environments.

Table 6. Primary Technology Focus in Included Studies (N = 73)

Technology Focus	Frequency	Percentage (%)	Analytical Insight
Zero Trust Architecture (ZTA Core)	23	32.0%	Core paradigm driving cybersecurity transformation
Identity and Access Management (IAM)	12	16.0%	Central to continuous verification mechanisms
Network Security & Micro-Segmentation	10	13.3%	Enables prevention of lateral movement
Cloud Security	8	10.7%	Supports distributed and remote environments
AI-driven Security / Automation	6	9.3%	Enhances predictive and adaptive risk management
IoT / Cyber-Physical Systems	6	8.0%	Expands attack surface and complexity
Governance, Risk & Compliance Tools	5	6.7%	Links security controls with governance outcomes
Blockchain / Emerging Technologies	3	4.0%	Emerging trust and audit mechanisms
Total	73	100%	

This demonstrates that Zero Trust operates as a socio-technical ecosystem integrating identity management, network segmentation, cloud security, and AI, rather than a standalone technical solution.

Synthesis of Study Characteristics

Collectively, the geographic, methodological, and technological characteristics of the included studies indicate a rapidly expanding field with increasing analytical sophistication. The convergence of diverse regional contexts, methodological approaches, and technological domains suggests that Zero Trust is evolving from a technical security model into a broader organizational paradigm integrating cybersecurity, risk management, and governance. Despite this evolution, the persistence of conceptual and methodological diversity reflects ongoing debates regarding implementation strategies, organizational readiness, and the translation of technical capabilities into governance outcomes. These characteristics provide a contextual foundation for interpreting thematic patterns and theoretical frameworks, with the PICO structure (Supplementary Table S1) ensuring consistent analysis of relationships between Zero Trust mechanisms and risk management outcomes.

Table 7. Major Barriers and Opportunity Themes (N = 73)

Theme	Key Subthemes	Studies (n)	Percentage (%)
Technical & Integration Barriers	Legacy systems integration, interoperability issues, system complexity, data heterogeneity, vendor lock-in	13	18.7%
Organizational & Cultural Barriers	Resistance to change, lack of security culture, leadership support, skill gaps, stakeholder misalignment	12	16.0%

Theme	Key Subthemes	Studies (n)	Percentage (%)
Economic & Resource Constraints	High implementation costs, limited budgets, lack of expertise, SME constraints, infrastructure limitations	10	13.3%
Governance & Regulatory Challenges	Compliance complexity (GDPR, ISO), lack of ZTA standards, audit difficulties, policy enforcement issues	8	10.7%
Security & Threat Landscape Challenges	Expanding attack surface (IoT/5G), advanced persistent threats (APT), supply chain vulnerabilities	6	8.0%
Opportunities: Advanced Risk Management & Security Enhancement	Lateral movement prevention, real-time threat detection, risk quantification, proactive defense mechanisms	10	14.7%
Opportunities: Governance, Compliance & Strategic Alignment	Improved regulatory compliance, continuous monitoring, audit automation, enterprise risk alignment	7	9.3%
Opportunities: Digital Transformation & Business Resilience	Process automation (RPA), improved decision-making, resilience frameworks, operational efficiency	4	5.3%
Opportunities: Integration with Emerging Technologies	AI-driven security, blockchain for trust, IoT protection, 5G/6G security, DevSecOps integration	3	4.0%
Total		73	100.0%

When considered collectively, temporal, geographic, methodological, and technological distributions reveal a clear pattern of rapid growth in publications, particularly after 2022, consistent across both the full dataset and core studies [36]; [37]; [38]. This growth is concentrated in regions with strong regulatory environments and is driven primarily by conceptual and technology-oriented research [36]; [39]; [40]. At the same time, identified barriers highlight persistent constraints related to technical complexity, organizational readiness, and regulatory fragmentation [4]; [41]. Conversely, emerging opportunities indicate the potential of Zero Trust to enhance risk management capabilities and strengthen governance alignment [42]; [4]. Overall, the evidence suggests that Zero Trust is simultaneously evolving as both a governance-driven and technology-driven paradigm, shaping cybersecurity practices and IT governance outcomes across diverse contexts [36]; [43].

3.2 Theoretical and Methodological Landscape

The theoretical foundations of the reviewed studies reveal a diverse and multi-layered intellectual structure. As summarized in Supplementary Table S13, Zero Trust Architecture (ZTA) represents the most dominant theoretical framework, followed by cyber risk management and quantification frameworks. Governance, compliance, and regulatory frameworks also play a significant role, reflecting the increasing integration of cybersecurity within broader organizational governance structures. In addition to these dominant perspectives, several complementary theoretical approaches are identified, including threat modeling frameworks (e.g., MITRE ATT&CK), maturity and capability models, and socio-technical frameworks emphasizing organizational culture and human factors. Emerging theoretical approaches, such as AI-driven security and blockchain-based trust frameworks, appear in a smaller subset of studies, indicating that these areas remain in an early stage of development. Methodologically, the dataset exhibits substantial heterogeneity, with conceptual and theoretical studies comprising the largest proportion (29.3%), followed by quantitative empirical studies (20.0%), qualitative analyses (16.0%), case studies (13.3%), mixed-methods designs (12.0%), and systematic reviews (9.3%) [31]; [44]. Analytical approaches vary accordingly, with structural equation modeling (SEM/PLS) widely used to examine relationships between organizational constructs and Zero Trust adoption, alongside regression analysis, Monte Carlo simulations, and network-based modeling techniques [45]; [46]. Multi-criteria decision-making approaches, particularly DEMATEL and entropy-based weighting methods, are frequently applied to evaluate interdependencies and prioritize implementation factors within complex cybersecurity environments [7]; [9]. Qualitative methodologies predominantly rely on thematic analysis, Delphi consensus techniques, and expert interviews, while systematic reviews consistently apply PRISMA-guided protocols to ensure methodological rigor [30]; [6]. Overall, these findings highlight a clear transition from purely technical security models toward integrated, multi-disciplinary perspectives combining technological, organizational, and governance dimensions.

3.3 Empirical Findings and Outcome Analysis

Across the reviewed studies, Zero Trust implementation is consistently treated as the primary independent construct, with outcomes measured through cybersecurity risk management, system performance, and

governance effectiveness [47]; [9]. Mediating factors commonly include continuous monitoring, identity verification, access control, and threat intelligence, whereas organizational maturity, regulatory frameworks, and technological complexity frequently act as moderating variables [4]; [3]. Primary outcomes include reduced attack surfaces, limited lateral movement, improved threat detection, and enhanced incident response [48]. Secondary outcomes relate to governance, including regulatory compliance, auditability, accountability, and standards alignment [12]; [32]. Emerging evidence further highlights AI- and blockchain-enabled capabilities that strengthen predictive analytics and automated security responses [15]; [49]. Quantitative findings consistently support Zero Trust adoption. Structural equation models report strong positive relationships between organizational factors and implementation success, with high reliability and validity across constructs [3]; [9]. Multi-criteria decision analyses also emphasize governance coordination and policy alignment as critical complements to technical controls. Overall, the evidence demonstrates robust positive associations between Zero Trust mechanisms and improved cybersecurity and governance outcomes across diverse contexts.

3.4 Risk Patterns and Quality Assessment

Risk assessments consistently identify external cyberattacks as the predominant threat across sectors [45]. Business and organizational environments exhibit greater vulnerability than educational or smaller-scale settings, while most organizations demonstrate moderate rather than high Zero Trust maturity [3]. Quality assessment using CASP and RoB 2 indicates a heterogeneous evidence base, comprising 15 strict-quality studies, 28 high-quality studies, 7 moderate-quality studies, and 25 studies with limited methodological rigor [27]. Although research objectives and methodological designs are generally well aligned, recurring limitations include sampling constraints and restricted external validity [50].

3.5 Technological and Data Considerations

Data limitations are mainly reported in SME-related and emerging technology studies, particularly due to the lack of longitudinal datasets [51]; [9]. Data heterogeneity and integration challenges are also frequently identified, especially in IoT and digital twin environments, where interoperability remains a key issue [30]. Technically, Zero Trust is implemented as a multi-layered architecture integrating identity management, network segmentation, cloud security, and AI-driven analytics [6]. These architectures typically include data collection, processing, and decision-making layers supported by machine learning and automated security mechanisms. AI techniques are widely used for anomaly detection, while blockchain is applied to enhance trust and data integrity in distributed systems [52]; [49], Supplementary Table 7.

Table 8. Technological Drivers of Risk Management and Governance in Zero Trust Environments

Technology Domain	Core Function in Zero Trust	Risk Management Impact	Governance Contribution
Artificial Intelligence (AI) & Automation	Behavioral analytics, anomaly detection, automated response	Proactive risk identification and adaptive threat mitigation	Data-driven decision-making and continuous monitoring
Blockchain / Distributed Ledger Technology	Decentralized trust, immutability, secure transactions	Integrity assurance and reduction of data tampering risks	Enhanced auditability, transparency, and trust
Cybersecurity Systems (ZTA Core, IAM, Segmentation)	Identity verification, access control, micro-segmentation	Reduction of attack surface and containment of lateral movement	Strengthened compliance and enforcement of security policies
Smart Infrastructure (IoT, Smart Cities)	Distributed device management, real-time monitoring	Management of complex and dynamic risk environments	Infrastructure governance and resilience enhancement
Digital Identity & Sovereignty	Identity-centric security, authentication, access governance	Mitigation of identity-based threats and unauthorized access	Regulatory compliance (GDPR, ISO) and accountability

3.6 Overall Synthesis of Evidence

The synthesis shows consistent positive relationships between Zero Trust implementation and cybersecurity risk management outcomes across the reviewed studies [53]; [39]; [43]. Zero Trust is commonly operationalized through mechanisms such as continuous authentication and least privilege access, while influenced by organizational and contextual factors [54]; [55]. However, variability is observed across

sectors, regions, and methodologies, particularly in the transition from perimeter-based to context-aware security models [42]; [43]. The evidence base is concentrated in technologically advanced regions, while SMEs and developing contexts remain underrepresented [43]. Key research gaps include limited longitudinal studies, insufficient SME-focused analysis, and a lack of standardized evaluation frameworks, as well as emerging areas such as generative AI and space cybersecurity [56]; [54]; [57].

3.7 Integrated Bibliometric and LDA Analysis

This section integrates bibliometric co-occurrence analysis and Latent Dirichlet Allocation (LDA) to provide a comprehensive interpretation of the cybersecurity research landscape. Bibliometric analysis identifies structural relationships among keywords, while LDA reveals latent thematic structures within documents, offering complementary perspectives on the field.

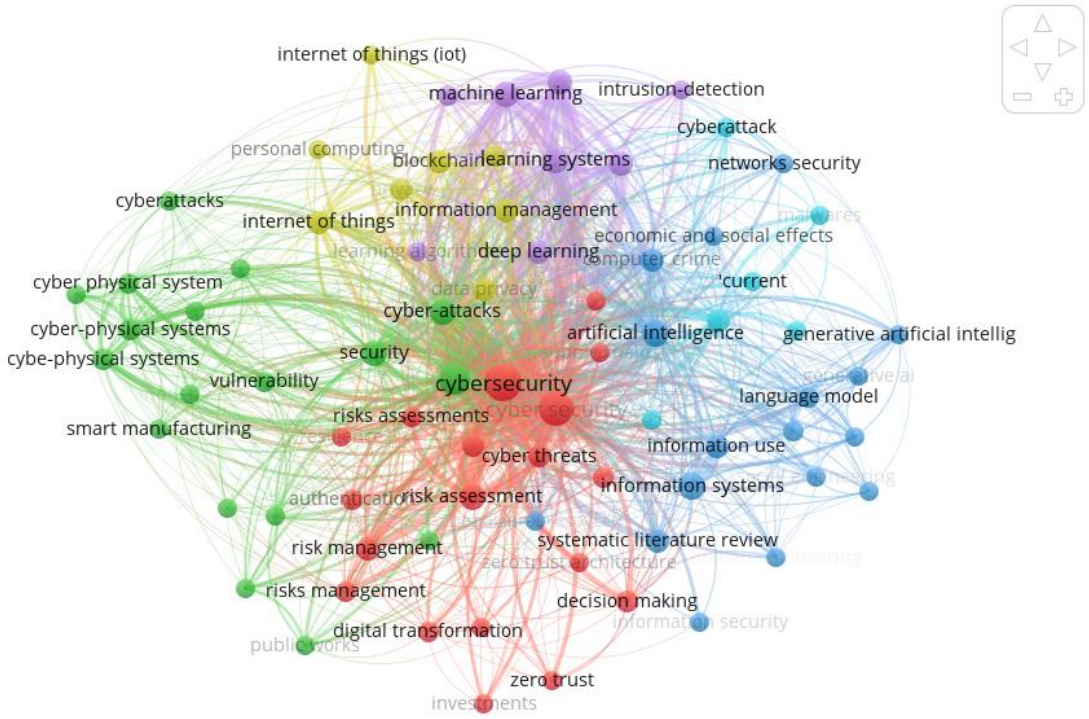


Figure 3. Keyword co-occurrence network of cybersecurity research themes

Bibliometric Co-occurrence Analysis of Keywords

A bibliometric co-occurrence analysis was conducted using VOSviewer to explore the intellectual structure of cybersecurity research in the context of artificial intelligence (AI) and emerging technologies. The dataset, extracted from Scopus-indexed publications, reveals a highly interconnected and evolving research landscape. The analysis identified four main thematic clusters.

Cluster 1: Core Cybersecurity and Risk Management

Keywords: cybersecurity, cyber threats, risk assessment, zero trust, decision making

This cluster represents the foundational cybersecurity domain, emphasizing risk management, decision-making, and the adoption of Zero Trust principles based on continuous verification.

Cluster 2: IoT and Cyber-Physical Systems

Keywords: internet of things, cyber-physical systems, smart manufacturing, vulnerability

This cluster highlights cybersecurity challenges in interconnected industrial and smart environments, particularly within Industry 4.0 systems.

Cluster 3: Artificial Intelligence and Advanced Computing

Keywords: artificial intelligence, generative AI, language model, information systems

This cluster reflects the integration of AI and advanced computing in cybersecurity, including both intelligent defense mechanisms and emerging AI-driven risks.

Cluster 4: Machine Learning and Data-Driven Approaches

Keywords: machine learning, deep learning, blockchain, intrusion detection

This cluster focuses on data-driven security techniques, including anomaly detection, intrusion detection, and decentralized trust mechanisms.

The results show a strongly interconnected structure, with cybersecurity acting as the central hub linking AI, IoT, blockchain, and risk management domains. This reflects the increasing convergence of intelligent computing technologies within cybersecurity research.

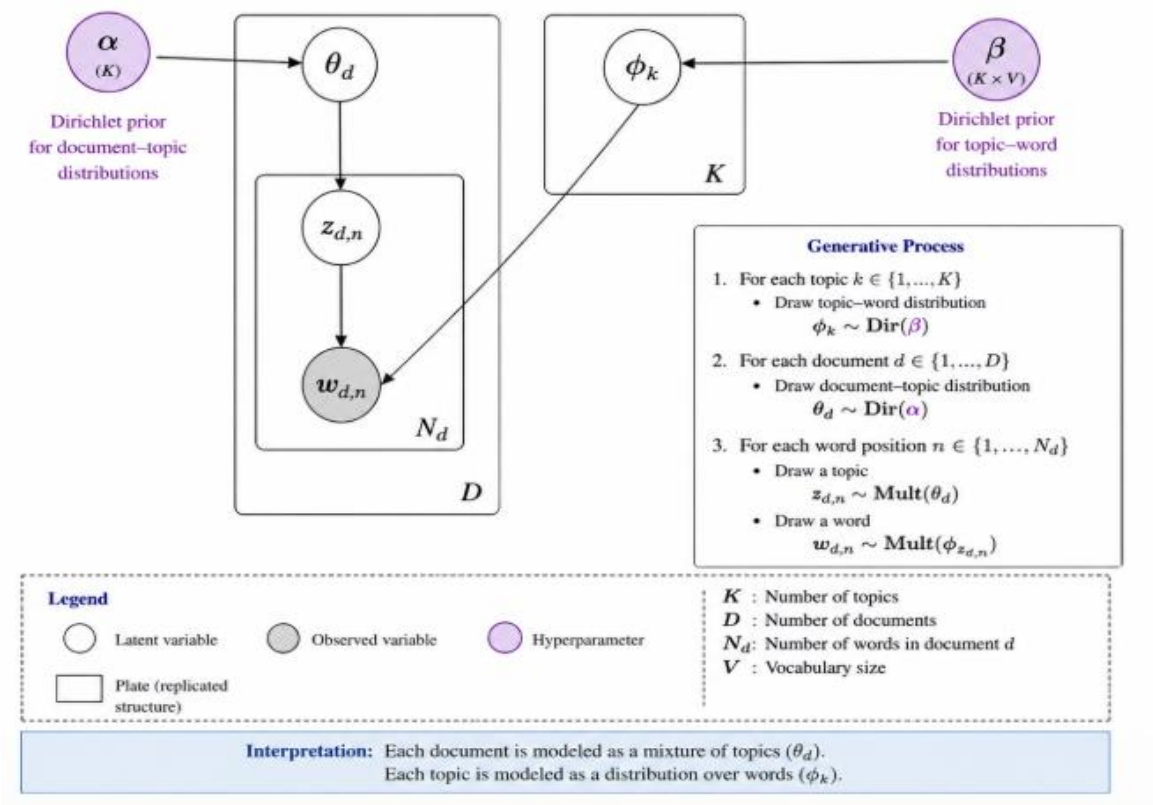


Figure 4. Latent Dirichlet Allocation (LDA) graphical model and generative process

Latent Dirichlet Allocation (LDA) Topic Modeling

To complement the bibliometric analysis and identify latent thematic structures, Latent Dirichlet Allocation (LDA) was applied to titles and abstracts [58]; [59]. LDA is a probabilistic topic modeling technique that represents each document as a mixture of topics and each topic as a distribution over words [55]. This approach is particularly suitable for cybersecurity research due to the coexistence of interdisciplinary themes such as AI, IoT, and risk management within the same literature [59]. The dataset was preprocessed using standard NLP techniques, including tokenization, stop-word removal, and lemmatization [60], to improve topic quality and interpretability. The model was implemented using Python (Gensim library), and the optimal number of topics (K) was selected based on coherence score evaluation. Model parameters (alpha

and beta) were tuned to improve topic sparsity and interpretability, and the model was iterated until convergence.

The analysis identified four main topics:

Topic 1: Cybersecurity Risk and Zero Trust

Keywords: cybersecurity, risk, zero trust, threats, assessment

This topic reflects the dominance of risk-based cybersecurity frameworks and Zero Trust architectures.

Topic 2: AI and Generative Security Systems

Keywords: artificial intelligence, generative AI, detection, prediction

This topic highlights the growing role of AI-driven cybersecurity and predictive security systems.

Topic 3: IoT and Cyber-Physical Systems

Keywords: IoT, smart systems, cyber-physical, vulnerability

This theme emphasizes security challenges in interconnected and industrial environments.

Topic 4: Data Management and Trust Systems

Keywords: information systems, blockchain, data privacy

This topic focuses on data integrity, trust management, and decentralized security mechanisms.

3.8 Integrated Interpretation of Bibliometric and LDA Results

The LDA results are consistent with the bibliometric clusters, confirming the robustness of the findings. Bibliometric analysis captures structural relationships among keywords, while LDA reveals deeper latent semantic patterns across documents, providing complementary perspectives on the cybersecurity research landscape.

4. Discussion

4.1. Paradigm Shift and Structural Drivers of Zero Trust Adoption

The literature indicates a fundamental shift from perimeter-based cybersecurity toward Zero Trust Architecture (ZTA), which establishes identity-centric governance based on continuous verification rather than implicit trust [27]; [61]. This reflects a broader transformation in which cybersecurity functions as a strategic governance mechanism embedded within organizational resilience, financial integrity, and business continuity, rather than a purely technical control function [47]; [62]. This shift is driven structurally by the "Extended Enterprise" model, where global supply chain interdependencies dissolve traditional organizational boundaries [5], and by Industry 4.0, which increases cyber-physical integration and expands the attack surface across interconnected systems [31]; [52]. Within this context, Digital Twins enhance decision intelligence through high-resolution transformation of sensor data [30], while AI-based systems support behavioral prediction and anomaly detection in complex environments [52]; [63]. However, Generative AI applications remain constrained by limited historical datasets in domains such as industrial IoT and space systems [14]; [51]. ZTA addresses these challenges by replacing perimeter defenses with continuous verification to protect organizational assets and reputation. Its adoption is accelerated by AI-driven security innovations but constrained by regulatory diversity and cloud complexity across regions [64]; [65]. Critical infrastructure sectors such as maritime transport and energy systems require domain-specific adaptation of Zero Trust principles. In maritime systems, standards such as IACS UR E26 operationalize least privilege access for onboard systems [21]. In energy grids, increasing IoT integration raises cybersecurity risks and necessitates stronger cyber resilience and skills development [66]. Additionally, supply chain vulnerabilities, as evidenced by incidents such as the SolarWinds breach, highlight the importance of continuous verification and Multi-Factor Authentication (MFA) as core safeguards [67]. For effectiveness, these controls must be embedded within hierarchical governance structures linking strategic,

tactical, and operational levels while ensuring continuous measurement of maturity and control effectiveness [68].

4.2. Organizational and Cultural Determinants of ZTA Adoption

The literature identifies organizational culture as the key determinant of Zero Trust Architecture (ZTA) success, with security culture and leadership commitment outweighing regulatory compliance, confirming ZTA as a socio-organizational transformation rather than a technical upgrade [3]. Mature organizations better embed continuous verification, while SMEs require phased implementation supported by MCDM and entropy-based models [61]; [6] to prioritize high-risk threats such as hacking and unauthorized access [45].

4.3. Methodological and Technological Convergence in Cybersecurity Systems

Research converges on hybrid frameworks integrating bibliometric analysis, PLS-SEM, DEMATEL, and entropy weighting [7]; [9]; [3], reflecting ZTA complexity. Technologically, ZTA integrates AI, ML, Blockchain, and Digital Twins to enable adaptive cybersecurity systems [17]; [69]; [49], though SME adoption remains limited due to resource constraints.

4.4. Systemic Cyber Risk Reconfiguration and Threat Dynamics

Cyber risk is increasingly systemic and network-based rather than isolated [46]. Heavy-tailed loss behavior challenges traditional risk models, pushing governance toward ecosystem-level approaches capable of managing cascading failures [46].

4.5. Theoretical, Governance, and Policy Implications

ZTA is explained through multiple theories: Principal-Agent (reducing information asymmetry) [9], RBV (strategic assets) [5]; [30], Institutional Theory (regulatory pressure) [47], and Socio-Technical Systems Theory (human–technology interaction) [70], framing ZTA as a hybrid governance architecture. Governance-wise, ZTA supports GDPR and HIPAA compliance but is insufficient alone [71]. Effective governance requires MITRE ATT&CK alignment, SBOM enforcement, and cryptographic supply chain verification [72]; [15]. Blockchain enhances trust in critical sectors [49]; [73], while ethical governance is needed to mitigate AI bias [15]; [69]. A shift is evident from financial loss-based models to trust-centric cybersecurity governance [62].

4.6. Research Gaps, Limitations, and Future Directions

Key gaps include limited integration of behavioral cybersecurity with AI-driven systems [9], lack of longitudinal studies in IoT and critical infrastructures [14], and geographic and methodological bias [47]; [31]. Future research should focus on AI-based incident prediction, cross-cultural ZTA adoption, decentralized identity in Industry 4.0, and longitudinal cybersecurity maturity models. Recommended methods include DSR, SmartPLS longitudinal analysis, and cross-country comparative studies [15]; [3].

Final Interpretation

Overall, the synthesis confirms that Zero Trust Architecture represents a foundational shift toward continuously verified, identity-centric cybersecurity governance. Its effectiveness depends not only on

technological sophistication but also on the alignment between organizational culture, regulatory structures, and adaptive technological systems. ZTA should therefore be understood as a dynamic socio-technical governance paradigm integrating AI, blockchain, and advanced analytics to achieve resilient digital ecosystems in the Industry 4.0 era [5].

5. Conceptual Framework for Zero Trust–Driven Cyber Risk Management and IT Governance

Building on the systematic synthesis of the reviewed studies, this research proposes an integrated conceptual framework explaining how Zero Trust Architecture (ZTA) influences cybersecurity risk management and IT governance within organizational information systems. The framework reflects a shift from perimeter-based security to a dynamic, data-driven model based on continuous verification, automation, and adaptive control.

It is derived from literature spanning 2020–2026, capturing both the emergence and evolution of Zero Trust into a comprehensive organizational strategy. In line with the PICO structure, organizational information systems represent the population, Zero Trust is the intervention, and outcomes include improved risk management, threat mitigation, regulatory compliance, and governance performance, while traditional security models serve as the implicit baseline for comparison. These mechanisms translate Zero Trust principles into measurable improvements in cybersecurity risk management, including enhanced threat detection, improved incident response, reduced lateral movement, and stronger mitigation strategies. The integration of frameworks such as NIST RMF and MITRE ATT&CK supports a shift from reactive to predictive risk management. Improvements in risk management subsequently extend to IT governance outcomes, reflected in stronger compliance, accountability, auditability, and alignment between cybersecurity and organizational strategy. The framework therefore establishes a sequential pathway in which ZTA influences security mechanisms, which enhance risk management, ultimately improving governance performance. In certain high-maturity organizations, direct effects of ZTA on risk management and governance are also observed; however, the literature indicates that mediated pathways are more consistent and dominant. The framework further identifies organizational maturity as a key moderating factor, influencing the effectiveness of implementation, while regulatory environments strengthen the translation of risk improvements into governance outcomes. Technologically, AI-driven analytics, behavioral monitoring, and automated response systems enhance real-time adaptation and continuous oversight, reinforcing the integration between operational security and governance. Overall, the framework provides a structured explanation of how ZTA drives cybersecurity transformation across strategic, operational, and governance levels, addressing a key gap in the literature by integrating these dimensions into a unified model.

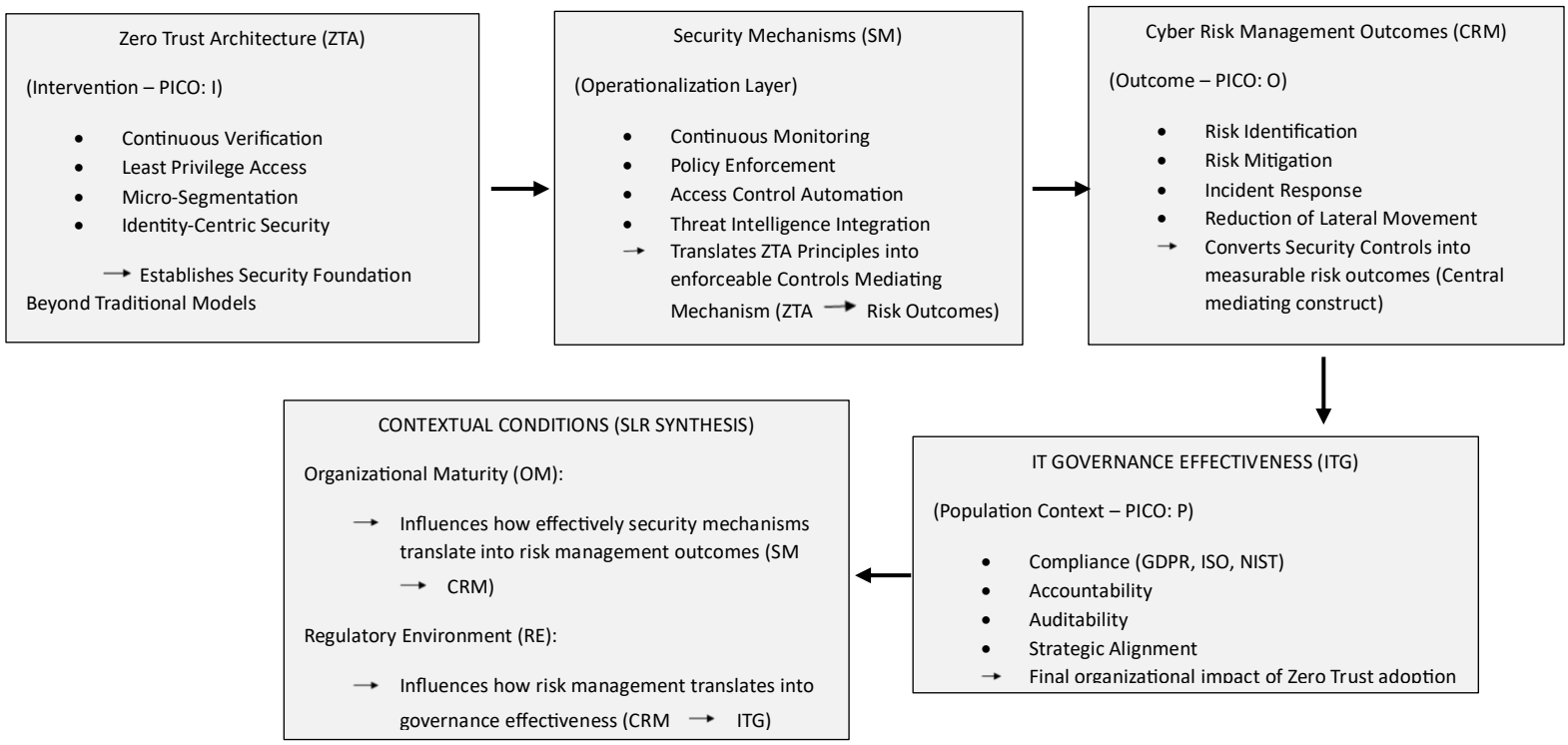


Figure 5. Zero Trust Impacts on Risk Management and IT Governance: A Systematic Review and Framework

Implications

This review positions Zero Trust as a socio-technical governance paradigm in which trust is continuously verified rather than assumed. Organizations should strengthen security culture, adopt phased risk-based implementation strategies, and integrate continuous monitoring into governance processes. Policymakers

should promote standardized Zero Trust maturity frameworks, automated compliance mechanisms, and supply chain security, with particular support for SMEs and developing regions. Future research should validate the proposed framework across diverse contexts and examine AI-driven security, decentralized identity, and governance challenges associated with generative AI. The review is limited by its inclusion of English-language studies, coverage up to Q1 2026, and the predominance of evidence from Europe, Asia-Pacific, and the MENA region.

Conclusion

The research establishes that Zero Trust Architecture (ZTA) represents a foundational shift toward a continuously verified and identity-centric governance model. This transition is not merely a technical adjustment but rather the emergence of a dynamic socio-technical paradigm where success is deeply contingent upon the alignment of organizational culture, leadership commitment, and adaptive technological systems. By serving as a critical mediating layer, the implementation of Zero Trust translates operational security controls into robust risk management capabilities, such as the mitigation of lateral movement and more proactive threat detection,. These advancements, in turn, enhance the effectiveness of IT governance by fostering superior regulatory compliance, accountability, and strategic alignment within the organization,. Furthermore, the study highlights a major conceptual evolution in how cyber risk is interpreted—moving from the perception of isolated incidents to the management of systemic and networked phenomena that require ecosystem-level management. As digital environments continue to grow in complexity, the integration of Zero Trust with emerging technologies like artificial intelligence, blockchain, and advanced analytics will be vital for achieving predictive defense and real-time risk mitigation. To fully realize this potential, future research and practice must address existing gaps by focusing on the development of longitudinal maturity models and ensuring the ethical governance of AI-driven cybersecurity systems.

Author Contributions: Conceptualization, Methodology, Software, Formal Analysis, Investigation, Data Curation, Writing – Original Draft, Supervision, and Project Administration were performed by the First Author, who conceived the hybrid methodological framework (SLR-bibliometric-LDA), performed computational analyses using VOSviewer, developed the integrative theoretical model, executed the systematic review and formal analysis, and drafted the original manuscript. Validation (including inter-rater reliability assessment, CASP quality appraisal, and thematic coherence verification) and Writing – Review & Editing were performed by the Second, Third, Fourth, Fifth, and Sixth Authors, who provided critical intellectual guidance, participated in data validation and thematic refinement, and revised the final manuscript. All authors have read and approved the submitted version. Funding acquisition: Not applicable.

Conflict of Interest

The author declares no financial, personal, or professional interest that might have influenced the research or the research outcomes.

Funding

No funding was provided by any individual, organization, or government entity.

Ethics Approval Statement

The authors argue this study does not require ethical approval since there were no human or animal experiments.

References

[1] V. Demertzi, S. Demertzis, and K. Demertzis, "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities," *Applied Sciences 2023, Vol. 13, Page 790*, vol. 13, no. 2, p. 790, Jan. 2023, doi: 10.3390/APP13020790.

[2] A. U. Patel *et al.*, "Cybersecurity and Information Assurance for the Clinical Laboratory," *J. Appl. Lab. Med.*, vol. 8, no. 1, pp. 145–161, Jan. 2023, doi: 10.1093/JALM/JFAC119.

[3] B. Zyoud and S. L. Lutfi, "The Role of Information Security Culture in Zero Trust Adoption: Insights From UAE Organizations," *IEEE Access*, vol. 12, pp. 72420–72444, 2024, doi: 10.1109/ACCESS.2024.3402341.

[4] A. Levine and B. A. Tucker, "Zero Trust Architecture: Risk Discussion," *Digital Threats: Research and Practice*, vol. 4, no. 1, Mar. 2023, doi: 10.1145/3573892;WGROUP:STRING:ACM.

[5] Z. A. Collier and J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," *Int. J. Prod. Res.*, vol. 59, no. 11, pp. 3430–3445, 2021, doi: 10.1080/00207543.2021.1884311.

[6] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," *Comput. Secur.*, vol. 133, p. 103412, Oct. 2023, doi: 10.1016/J.COSE.2023.103412.

[7] A. A. Alarood and A. O. Alzahrani, "Interoperable Defensive Strategies of Network Security Evaluation," *IEEE Access*, vol. 12, pp. 33959–33971, 2024, doi: 10.1109/ACCESS.2024.3373710.

[8] B. Chen *et al.*, "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," *IEEE Internet Things J.*, vol. 8, no. 13, p. 10248, Jul. 2020, doi: 10.1109/JIOT.2020.3041042.

[9] A. Pigola, F. de Souza Meirelles, and P. R. da Costa, "Trust Management in the Age of Zero trust: a comprehensive multi-method analysis from enterprise challenges," *Enterp. Inf. Syst.*, vol. 20, no. 1, 2026, doi: 10.1080/17517575.2025.2588753.

[10] A. Chaudhuri and S. Bozkus Kahyaoglu, "CYBERSECURITY ASSURANCE IN SMART CITIES: A RISK MANAGEMENT PERSPECTIVE," *EDPACS*, vol. 67, no. 4, pp. 1–22, Apr. 2023, doi: 10.1080/07366981.2023.2165293.

[11] B. Metin, S. Duran, E. Telli, M. Mutlutürk, and M. Wynn, "IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture," *Information (Switzerland)*, vol. 15, no. 1, Jan. 2024, doi: 10.3390/info15010055.

[12] D. David and S. Ferguson, "The outcome efficacy of the entity risk management requirements of the NIS 2 Directive," *International Cybersecurity Law Review 2023 4:4*, vol. 4, no. 4, pp. 371–386, Aug. 2023, doi: 10.1365/S43439-023-00097-8.

[13] K. Kepuska and M. Tomasevic, "A lightweight framework for cyber risk management in Western Balkan higher education institutions," *PeerJ Comput. Sci.*, vol. 10, pp. 1–23, 2024, doi: 10.7717/peerj-cs.1958.

[14] S. L. Mirtaheri, N. Movahed, R. Shahbazian, V. Pascucci, and A. Pugliese, "Cybersecurity in the age of generative AI: A systematic taxonomy of AI-powered vulnerability assessment and risk management," *Future Generation Computer Systems*, vol. 175, p. 108107, Feb. 2026, doi: 10.1016/J.FUTURE.2025.108107.

[15] I. Coston, K. D. Hezel, E. Plotnizky, and M. Nojoumian, "Enhancing Secure Software Development with AZTRM-D: An AI-Integrated Approach Combining DevSecOps, Risk Management, and Zero Trust," *Applied Sciences 2025, Vol. 15, Page 8163*, vol. 15, no. 15, p. 8163, Jul. 2025, doi: 10.3390/APP15158163.

[16] M. Salayma, "Risk and threat mitigation techniques in internet of things (IoT) environments: a survey," *Frontiers in the Internet of Things*, vol. 2, p. 1306018, Jan. 2024, doi: 10.3389/FRIOT.2023.1306018/TEXT.

[17] B. Al-Sada, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the Art and Way Forward," *ACM Comput. Surv.*, vol. 57, no. 1, Oct. 2024, doi: 10.1145/3687300.

[18] R. O. Andrade, S. G. Yoo, I. Ortiz-Garces, and J. Barriga, "Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices," *Applied Sciences 2022, Vol. 12, Page 2976*, vol. 12, no. 6, p. 2976, Mar. 2022, doi: 10.3390/APP12062976.

[19] J. M. Lee, M. S. Sim, Y. S. Kim, H. R. Lim, and C. H. Lee, "Strategizing Artificial Intelligence Transformation in Smart Ports: Lessons from Busan's Resilient AI Governance Model," *Journal of Marine Science and Engineering 2025, Vol. 13, Page 1276*, vol. 13, no. 7, p. 1276, Jun. 2025, doi: 10.3390/JMSE13071276.

[20] Í. Oliveira, T. P. Sales, J. P. A. Almeida, R. Baratella, M. Fumagalli, and G. Guizzardi, "Ontology-based security modeling in ArchiMate," *Softw. Syst. Model.*, vol. 23, no. 4, pp. 925–952, Aug. 2024, doi: 10.1007/s10270-024-01149-1.

[21] G. Kayisoglu, E. Duzenli, P. Bolat, and F. Bolat, "Maritime Cyber Security: Adopting a Checklist Based on IACS UR E26 Standard," *Turkish Journal of Maritime and Marine Sciences*, vol. 10, no. Özel Sayı: 1, pp. 31–50, Oct. 2024, doi: 10.52998/trjmms.1531150.

[22] B. Linan-Acosta, O. Bazalar-Gonzales, and J. Santisteban, "GuardNet: An Architecture Based on NIST v2.0 for Confidential Data Protection in Higher Education Institutions in Peru," *Engineering, Technology & Applied Science Research*, vol. 15, no. 6, pp. 28977–28985, Dec. 2025, doi: 10.48084/ETASR.12978.

[23] L. S. Hsiao, I. L. Lin, C. J. Huang, and H. Te Liu, "Analysis of Factors Influencing Cybersecurity in Railway Critical Infrastructure: A Case Study of Taiwan Railway Corporation, Ltd.," *Systems 2025, Vol. 13, Page 861*, vol. 13, no. 10, p. 861, Sep. 2025, doi: 10.3390/SYSTEMS13100861.

[24] M. Sadeghiravesh, … H. K.-A. P., and undefined 2021, "Fuzzy logic model to assess desertification intensity based on vulnerability indices," *real-j.mtak.huMH Sadeghiravesh, H Khosravi, A Abolhasani, M Ghodsi, A MosaviActa Polytechnica Hungarica, 2021•real-j.mtak.hu*, 2021, Accessed: Apr. 22, 2026. [Online]. Available: http://real-j.mtak.hu/21037/3/APH_2021_18_03_.pdf

[25] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting Zero Trust Network Architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, pp. 1309–1320, Nov. 2022, doi: 10.1016/J.EGYR.2021.11.272.

[26] O. I. Falowo, M. Ozer, C. Li, and J. B. Abdo, "Evolving Malware and DDoS Attacks: Decadal Longitudinal Study," *IEEE Access*, vol. 12, pp. 39221–39237, 2024, doi: 10.1109/ACCESS.2024.3376682.

[27] 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.

[28] H. Silva, M. Vieira, and A. Neto, "A Survey on Survivable Safety-Critical Systems," *IEEE Access*, vol. 13, pp. 127770–127787, 2025, doi: 10.1109/ACCESS.2025.3590244.

[29] H. Tharwat, S. T. Hafez, I. E. Elgohary, and A. Hassanein, "A decade of cybersecurity research in internal auditing: bibliometric mapping and future research agenda," *Discover Sustainability 2025 6:1*, vol. 6, no. 1, pp. 1066-, Oct. 2025, doi: 10.1007/S43621-025-02031-W.

[30] O. Hakimi, H. Liu, O. Abudayyeh, A. Houshyar, M. Almatared, and A. Alhawiti, "Data Fusion for Smart Civil Infrastructure Management: A Conceptual Digital Twin Framework," *Buildings 2023, Vol. 13, Page 2725*, vol. 13, no. 11, p. 2725, Oct. 2023, doi: 10.3390/BUILDINGS13112725.

[31] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors 2023, Vol. 23, Page 6666*, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/S23156666.

[32] R. Vanickova, "SYSTEMATIZATION OF PROCESSES OF VALUE-CREATING ACTIVITIES OF OPERATIONAL SUSTAINABILITY AND SOCIAL RESPONSIBILITY," *Economics and Culture*, vol. 21, no. 2, pp. 199–224, Dec. 2024, doi: 10.2478/jec-2024-0028.

[33] A. M. Algarni and V. Thayananthan, "Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model," *IEEE Access*, vol. 11, pp. 15284–15296, 2023, doi: 10.1109/ACCESS.2023.3244883.

[34] S. O. Oruma and S. Petrovic, "Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey," *IEEE Access*, vol. 11, pp. 63205–63237, 2023, doi: 10.1109/ACCESS.2023.3288338.

[35] M. Marques, V. Delgado-Gomes, F. Januário, C. Lopes, R. Jardim-Goncalves, and C. Agostinho, "The B-Health Box: A Standards-Based Fog IoT Gateway for Interoperable Health and Wellbeing Data Collection," *Sensors 2025, Vol. 25, Page 7116*, vol. 25, no. 23, p. 7116, Nov. 2025, doi: 10.3390/S25237116.

[36] F. Casaril and L. Galletta, "Space cybersecurity governance: assessing policies and frameworks in view of the future European space legislation," *J. Cybersecur.*, vol. 11, no. 1, p. 13, Jan. 2025, doi: 10.1093/CYBSEC/TYAF013.

[37] A. Harkai and C. E. Ciurea, "Economic impact of IOT and conventional data breaches: cost analysis and statistical trends," *Control and Cybernetics*, vol. 53, no. 2, pp. 385–404, Jun. 2024, doi: 10.2478/candc-2024-0017.

[38] A. Kurylets and N. Goranin, "Security Ontology OntoSecRPA for Robotic Process Automation Domain," *Applied Sciences 2023, Vol. 13, Page 5568*, vol. 13, no. 9, p. 5568, Apr. 2023, doi: 10.3390/APP13095568.

[39] J. Horalek and V. Sobeslav, "Security Baseline for Substation Automation Systems," *Sensors 2023, Vol. 23, Page 7125*, vol. 23, no. 16, p. 7125, Aug. 2023, doi: 10.3390/S23167125.

[40] L. Mocean and M.-P. Vlad, "Security Ontology in a Virtual University," *Land Forces Academy Review*, vol. 29, no. 2, pp. 161–170, Jun. 2024, doi: 10.2478/raft-2024-0017.

[41] C. Neale, I. Kennedy, B. Price, Y. Yu, and B. Nuseibeh, "The case for Zero Trust Digital Forensics," *Forensic Science International: Digital Investigation*, vol. 40, p. 301352, Mar. 2022, doi: 10.1016/J.FSIDI.2022.301352.

[42] L. Alevizos and E. Stavrou, "Cyber threat modeling for protecting the crown jewels in the Financial Services Sector (FSS)," *Information Security Journal: A Global Perspective*, vol. 32, no. 2, pp. 134–161, Mar. 2023, doi: 10.1080/19393555.2022.2104766.

[43] M. Karpiuk, W. Pizło, and K. Kaczmarek, "CYBERSECURITY MANAGEMENT – CURRENT STATE AND DIRECTIONS OF CHANGE," *International Journal of Legal Studies (IJOLS)*, vol. 14, no. 2, pp. 645–663, Dec. 2023, doi: 10.5604/01.3001.0054.2880.

[44] S. Almarri and A. Aljughaiman, "Blockchain Technology for IoT Security and Trust: A Comprehensive SLR," Dec. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/su162310177.

[45] A. Zadeh, B. Lavine, H. Zolbanin, and D. Hopkins, "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions," *Decision Analytics Journal*, vol. 9, p. 100328, Dec. 2023, doi: 10.1016/J.DAJOUR.2023.100328.

[46] R. Pal, R. X. Sequeira, X. Yin, S. Zeijlemaker, and V. Kotala, "How Should Enterprises Quantify and Analyze (Multi-Party) APT Cyber-Risk Exposure in their Industrial IoT Network?," *ACM Trans. Manag. Inf. Syst.*, Oct. 2023, doi: 10.1145/3605949.

[47] Q. H. Pham and K. P. Vu, "Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises," *Cogent Business and Management*, vol. 11, no. 1, 2024, doi: 10.1080/23311975.2024.2364053.

[48] H. El Amin, A. E. Samhat, M. Chamoun, L. Oueidat, and A. Feghali, "An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure," *Journal of Cybersecurity and Privacy 2024, Vol. 4, Pages 357-381*, vol. 4, no. 2, pp. 357–381, Jun. 2024, doi: 10.3390/JCP4020018.

[49] H. Moosa, M. Ali, H. Alaswad, W. Elmedany, and C. Balakrishna, "A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing," *Arab J. Basic Appl. Sci.*, vol. 30, no. 1, pp. 179–196, Dec. 2023, doi: 10.1080/25765299.2023.2188701.

[50] J. A. Gómez Hernández, P. García Teodoro, R. Magán Carrión, and R. Rodríguez Gómez, "Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges," *Electronics 2023, Vol. 12, Page 4494*, vol. 12, no. 21, p. 4494, Nov. 2023, doi: 10.3390/ELECTRONICS12214494.

[51] S. Shahzad, K. Joiner, L. Qiao, F. Deane, and J. Plested, "Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers," *Systems 2024, Vol. 12, Page 434*, vol. 12, no. 10, p. 434, Oct. 2024, doi: 10.3390/SYSTEMS12100434.

[52] R. Verma, S. Koul, and K. V. Ajaygopal, "Evaluation and Selection of a Cybersecurity Platform Case of the Power Sector in India," *Decision Making: Applications in Management and Engineering*, vol. 7, no. 1, pp. 209–236, Apr. 2024, doi: 10.31181/dmame712024891.

[53] E. Adams, J. Bischoff, and M. Erdem, "'High-Stakes' Security: Current and Emerging Trends in Casino Gaming Cybersecurity," *UNLV Gaming Research & Review Journal*, vol. 29, no. 1, Sep. 2025, doi: 10.9741/2327-8455.1506.

[54] L. Li, L. Liu, and L. Xiang, "Optimisation and application of management accounting system based on generative artificial intelligence," *International Journal of Information and Communication Technology*, vol. 26, no. 27, pp. 1–21, 2025, doi: 10.1504/IJICT.2025.147530.

[55] Z. Zhang *et al.*, "MTTEGDM: A Moving Target Evolutionary Game Defense Model Based on Three-Way Decisions," *Electronics 2024, Vol. 13, Page 734*, vol. 13, no. 4, p. 734, Feb. 2024, doi: 10.3390/ELECTRONICS13040734.

[56] W. F. Cosgrove and W. F. Cosgrove, "Technology: The Air and Space Force's Barrier to Innovation," *Space and Defense*, vol. 14, no. 1, p. 5, Oct. 2023, doi: 10.32873/uno.dc.sd.14.01.1049.

[57] N. Y. Xu *et al.*, "The Launch of the iCoDE Standard Project," *J. Diabetes Sci. Technol.*, vol. 16, no. 4, pp. 887–895, Jul. 2022, doi: 10.1177/19322968221093662;

[58] Huang ; Wang, "The Devastating Business Impacts of a Cyber Breach." Accessed: Apr. 10, 2026. [Online]. Available: https://cams.mit.edu/wp content/uploads/2023-05-04-HBR-The-Devastating-Business-Impacts-of-a-Cyber-Breach84.pdf.

[59] M. Jofre *et al.*, "Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach," *Applied Sciences 2021, Vol. 11, Page 6699*, vol. 11, no. 15, p. 6699, Jul. 2021, doi: 10.3390/APP11156699.

[60] C. Li, "Application of nonlinear recursion equation in network security risk detection," *Nonlinear Engineering*, vol. 11, no. 1, pp. 437–446, Jan. 2022, doi: 10.1515/NLENG-2022-0220/XML.

[61] S. Pawar and H. Palivela, "NEED OF PARADIGM SHIFT IN CYBERSECURITY IMPLEMENTATION FOR SMALL AND MEDIUM ENTERPRISES (SMES)," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 8, no. 1, Apr. 2025, doi: 10.52306/2578-3289.1184.

[62] S. Perera, X. Jin, A. Maurushat, and D. G. J. Opoku, "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks," *Informatics 2022, Vol. 9, Page 28*, vol. 9, no. 1, p. 28, Mar. 2022, doi: 10.3390/INFORMATICS9010028.

[63] S. Mohammed, S. Nanthini, N. Bala Krishna, I. V. Srinivas, M. Rajagopal, and M. Ashok Kumar, "A new lightweight data security system for data security in the cloud computing," *Measurement: Sensors*, vol. 29, p. 100856, Oct. 2023, doi: 10.1016/J.MEASEN.2023.100856.

[64] M. W. Hodgins, "The cybersecurity entrepreneur," *The Review of Austrian Economics 2024 38:3*, vol. 38, no. 3, pp. 265–286, May 2025, doi: 10.1007/S11138-024-00641-7.

[65] O. Ogasawara, "Building cloud computing environments for genome analysis in Japan," *Human Genome Variation 2022 9:1*, vol. 9, no. 1, pp. 46-, Dec. 2022, doi: 10.1038/s41439-022-00223-8.

[66] R. Pirta-Dreimane *et al.*, "Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation," *Energies 2024, Vol. 17, Page 1876*, vol. 17, no. 8, p. 1876, Apr. 2024, doi: 10.3390/EN17081876.

[67] J. Martí Nez and J. M. Durá, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study," *International Journal of Safety and Security Engineering*, vol. 11, Sep. 2021, doi: 10.18280/ijsse.110505.

[68] M. Liu, M. Shore, W. Yeoh, F. Jiang, and S. Zeadally, "Toward effective cybersecurity management: a hierarchical process model with performance assessment," *J. Cybersecur.*, vol. 11, no. 1, p. 20, Jan. 2025, doi: 10.1093/CYBSEC/TYAF020.

[69] J. Liu, T. Han, J. Zhao, D. Mu, H. Liu, and B. Tang, "An Intelligent Risk Assessment Methodology for the Full Lifecycle Security of Data," *Symmetry 2025, Vol. 17, Page 820*, vol. 17, no. 6, p. 820, May 2025, doi: 10.3390/SYM17060820.

[70] S. Siddique *et al.*, "An effective framework to improve the managerial activities in global software development," *Nonlinear Engineering*, vol. 12, no. 1, Jan. 2023, doi: 10.1515/NLENG-2022-0312/XML.

[71] C. Regueiro and B. Urquizu, "Blockchain-Based Evidence Trustworthiness System in Certification," *Journal of Cybersecurity and Privacy 2025, Vol. 5, Page 1*, vol. 5, no. 1, p. 1, Dec. 2024, doi: 10.3390/JCP5010001.

[72] A. Adem, E. Çakıt, M. Dağdeviren, B. Mrugalska, and W. Karwowski, "Understanding security challenges in the software supply chain through causal relationships," *PLoS One*, vol. 21, no. 3, p. e0344098, Mar. 2026, doi: 10.1371/JOURNAL.PONE.0344098.

[73] A. Puder, J. Henle, and E. Sax, "Threat Assessment and Risk Analysis (TARA) for Interoperable Medical Devices in the Operating Room Inspired by the Automotive Industry," *Healthcare 2023, Vol. 11, Page 872*, vol. 11, no. 6, p. 872, Mar. 2023, doi: 10.3390/HEALTHCARE11060872.