Review of Applied Science and Technology

Volume: 1; Issue: 4
Pages: 323– 374

# Zero-Trust Architecture Adoption on Financial Data Privacy in Public-Sector ERP Environments

**S M Arif Al Sany[1]; Siful Islam[2]**

[1]. Senior Executive in Finance, Jatra Solutions, MGH Group, Dhaka, Bangladesh; Email: alsany25@gmail.com

[2]. Bachelor of Science in Computer Science and Engineering, Bangladesh University of Business & Technology, Dhaka, Bangladesh; Email: sifulbubt@gmail.com

Doi: 10.63125/j8cas279
**Received:** 15 September 2022; **Revised:** 18 October 2022; **Accepted:** 15 November 2022; **Published:** 06 December 2022;

## Abstract

*The increasing dependence on Enterprise Resource Planning systems within public-sector institutions has intensified concerns regarding cybersecurity governance, financial data privacy, and protection of sensitive governmental information against evolving cyber threats. This study examined the influence of Zero-Trust Architecture adoption on financial data privacy performance within public-sector ERP environments. The study adopted a quantitative cross-sectional research design grounded in Zero-Trust Security Theory and Information Security Governance Theory. Data were collected from 312 cybersecurity professionals, ERP administrators, IT managers, compliance officers, and digital governance personnel working across ministries, treasury departments, taxation agencies, procurement authorities, municipal administrations, and pension management institutions utilizing ERP systems for financial management operations. Structured questionnaires measured identity governance implementation, multi-factor authentication usage, network segmentation practices, continuous monitoring technologies, access governance effectiveness, and financial data privacy performance. Data analysis was conducted using descriptive statistics, Pearson correlation analysis, and multiple regression analysis through the Statistical Package for the Social Sciences software. The findings demonstrated high implementation levels of multi-factor authentication systems ($M = 4.35$, $SD = 0.58$), identity governance frameworks ($M = 4.28$, $SD = 0.63$), and continuous monitoring technologies ($M = 4.18$, $SD = 0.71$) across participating institutions. Correlation analysis revealed strong positive relationships between identity governance frameworks and financial information confidentiality ($r = 0.812$, $p < 0.01$), while multi-factor authentication showed significant association with unauthorized access prevention capability ($r = 0.825$, $p < 0.01$). Multiple regression analysis further indicated that identity governance frameworks ($\beta = 0.384$, $p = 0.000$) and multi-factor authentication systems ($\beta = 0.331$, $p = 0.000$) significantly predicted financial data privacy performance within governmental ERP systems. The regression model explained 71.8% of the variance associated with financial data privacy outcomes ($R^2 = 0.718$). The findings established that Zero-Trust Architecture significantly strengthened ERP cybersecurity governance, improved institutional resilience, enhanced confidentiality protection, and reduced operational exposure to unauthorized access incidents affecting public-sector financial information systems.*

## Keywords

*Zero-Trust Architecture, ERP Security, Financial Data Privacy, Cybersecurity Governance, Public-Sector Systems.*

## INTRODUCTION

Enterprise Resource Planning systems represent integrated digital infrastructures that centralize organizational data, automate operational workflows, and coordinate institutional activities across finance, procurement, human resources, budgeting, and governance functions. In public-sector institutions, ERP environments function as strategic platforms for managing national assets, taxation systems, citizen records, procurement activities, and financial reporting procedures. The increasing digitization of governmental operations has elevated ERP systems from administrative utilities into mission-critical infrastructures that support economic stability, regulatory compliance, and public accountability (Di Salvo, 2018). Financial data privacy within these systems has therefore emerged as a central concern for governments, international regulatory bodies, and cybersecurity agencies. Public-sector institutions routinely process confidential financial information involving public expenditures, taxpayer transactions, pension systems, payroll databases, banking records, and interdepartmental financial transfers.

**Figure 1: ERP system diagram and modules**


Unauthorized access to such information can generate severe economic disruption, institutional distrust, corruption vulnerabilities, and geopolitical risks. The expansion of remote access technologies, cloud-based ERP deployment models, and interconnected digital governance frameworks has intensified exposure to cyber threats targeting sensitive governmental financial assets. Traditional perimeter-based cybersecurity models have become increasingly insufficient because contemporary cyberattacks frequently exploit insider threats, credential compromise, lateral network movement, and unauthorized privilege escalation (Albuquerque et al., 2014). In response to these evolving challenges, Zero-Trust Architecture has emerged as a cybersecurity framework centered on continuous verification, least-privilege access control, identity authentication, network segmentation, and persistent monitoring mechanisms. The conceptual foundation of Zero-Trust Architecture rejects assumptions of automatic trust within internal organizational networks and instead requires validation for every user, device, application, and transaction attempting access to organizational resources. International cybersecurity agencies, including governmental digital security authorities and financial oversight institutions, have increasingly recognized Zero-Trust principles as essential for protecting

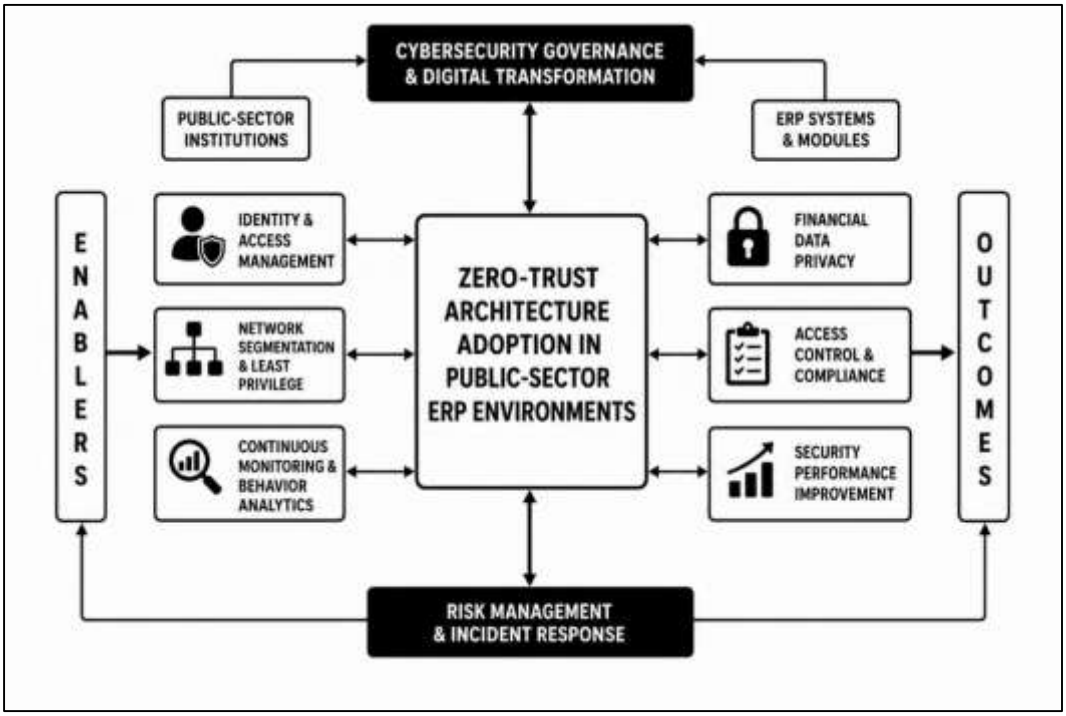
sensitive financial systems. Public-sector ERP environments have consequently become important domains for examining how Zero-Trust adoption influences financial data privacy outcomes, cybersecurity resilience, access governance, and institutional protection strategies (Golam & Amir, 2022; Abdur & Iftekhar, 2021; Weiss, 2020). The growing frequency of ransomware attacks, financial data breaches, and state-sponsored cyber intrusions across governmental institutions has transformed cybersecurity from a technical concern into a multidimensional issue involving economic security, public trust, administrative continuity, and national governance stability.

The global significance of cybersecurity within public-sector ERP environments has expanded alongside rapid digital transformation initiatives implemented across both developed and emerging economies. Governments increasingly rely on centralized ERP infrastructures to support digital taxation, public budgeting, electronic procurement, welfare distribution, infrastructure financing, healthcare administration, and educational funding systems. These transformations have generated substantial efficiency improvements while simultaneously increasing exposure to sophisticated cyber threats targeting public financial ecosystems (Blum, 2020). International organizations concerned with financial integrity and digital governance have reported significant growth in cyber incidents affecting public institutions responsible for financial administration. Financially motivated cybercriminals, politically driven hacking groups, and advanced persistent threat actors increasingly target governmental databases because of the strategic value of public financial information. ERP systems within ministries, treasury departments, municipal authorities, and regulatory agencies contain interconnected repositories of sensitive records that can be exploited for fraud, extortion, espionage, or systemic disruption (Atif & Murad, 2022; Binayan & Shakhawat, 2022). The interconnected nature of public-sector ERP platforms amplifies the consequences of unauthorized access because a single compromised credential may permit extensive movement across institutional networks. This operational complexity has encouraged governments to reconsider traditional cybersecurity frameworks based on implicit internal trust assumptions (Setiawan et al., 2016). Zero-Trust Architecture introduces a fundamentally different approach by treating all access requests as potentially hostile until authenticated through contextual verification mechanisms. Such mechanisms often include multi-factor authentication, behavioral analytics, identity governance protocols, endpoint verification, encryption policies, and real-time access monitoring. The increasing adoption of hybrid work arrangements, cross-agency collaboration platforms, and cloud-hosted governmental ERP solutions has further strengthened the importance of continuous identity validation and adaptive security policies. Public institutions operating within financially constrained environments face additional challenges because legacy systems, fragmented infrastructure, and inconsistent cybersecurity governance can weaken privacy protections (Sokolov et al., 2014). Quantitative investigation into the adoption of Zero-Trust frameworks therefore becomes essential for understanding measurable relationships between cybersecurity architecture and financial data privacy outcomes. Such investigations support evidence-based analysis regarding whether Zero-Trust implementation improves confidentiality controls, reduces unauthorized access incidents, strengthens access governance, and enhances institutional protection within public-sector ERP ecosystems.

Financial data privacy constitutes a multidimensional concept involving the protection of sensitive monetary information from unauthorized disclosure, misuse, manipulation, theft, or exploitation. Within public-sector ERP environments, financial data privacy extends beyond technical confidentiality and encompasses institutional accountability, citizen trust, ethical governance, and compliance with national regulatory standards (Henman, 2020). Public-sector financial databases commonly include payroll records, tax information, procurement contracts, banking transactions, pension contributions, debt obligations, and intergovernmental financial exchanges. Exposure of such information can compromise public confidence, disrupt economic operations, weaken governance credibility, and create opportunities for financial corruption or fraud. The expansion of digital government initiatives has increased dependence on centralized ERP infrastructures that aggregate extensive volumes of confidential financial information across interconnected departments and agencies. This aggregation strengthens operational efficiency while simultaneously increasing systemic vulnerability because attackers may gain access to broad categories of sensitive data through a single compromised access point. Traditional cybersecurity strategies often rely on static perimeter defenses

such as firewalls and internal network trust assumptions. Contemporary cyber threats increasingly circumvent these approaches through phishing campaigns, credential theft, social engineering, insider misuse, and exploitation of privileged accounts (Srinivas & Vivek, 2014).

**Figure 2: Zero-trust architecture in public-sector ERP**




Zero-Trust Architecture addresses these weaknesses by integrating identity-centric security models that continuously validate users and devices regardless of their network location. Continuous authentication mechanisms, role-based access restrictions, micro-segmentation policies, and anomaly detection systems collectively support stronger privacy controls within ERP infrastructures. The adoption of Zero-Trust principles has become particularly relevant within public administration because governmental institutions frequently operate under complex legal obligations related to financial transparency and citizen data protection. Digital governance reforms implemented across various nations have emphasized the importance of secure information management systems capable of protecting confidential financial assets while maintaining operational accessibility. Quantitative evaluation of Zero-Trust adoption within ERP systems can therefore provide empirical insight into measurable privacy outcomes such as reductions in unauthorized access frequency, improvements in compliance performance, strengthened user authentication effectiveness, and enhanced control over financial information exposure (Nanos et al., 2018). Such investigation contributes to broader understanding regarding the effectiveness of cybersecurity modernization strategies within high-risk public financial environments characterized by expanding digital dependency and escalating cyber vulnerability.

Zero-Trust Architecture emerged as a response to structural weaknesses associated with traditional network security models that assumed internal organizational environments were inherently trustworthy. Conventional cybersecurity approaches focused heavily on perimeter defense mechanisms designed to prevent external intrusions while granting broad internal access privileges to authenticated users (Sarwar et al., 2019). This security philosophy became increasingly ineffective as organizations adopted cloud computing, mobile technologies, remote access systems, and interconnected digital infrastructures. Modern cyberattacks frequently originate from compromised internal accounts, malicious insiders, third-party vendors, or attackers who gain initial entry through stolen credentials. Zero-Trust Architecture addresses these vulnerabilities through a framework centered on continuous verification, explicit authentication, least-privilege access enforcement, and

persistent activity monitoring. The architecture operates according to the principle that trust should never be automatically granted based on network location or user status. Instead, every access request must be continuously validated through contextual analysis involving user identity, device condition, behavioral patterns, geolocation, access timing, and resource sensitivity. Public-sector ERP systems represent ideal environments for examining the operational impact of Zero-Trust implementation because they involve extensive user populations, interconnected databases, and high-value financial information assets (Seo & Myeong, 2020). Government agencies frequently support thousands of employees, contractors, vendors, and administrators requiring varying degrees of system access across multiple departments and jurisdictions. This complexity creates significant challenges related to identity governance, privilege management, and unauthorized access prevention. Zero-Trust frameworks introduce segmented access structures that limit unnecessary user permissions and restrict lateral network movement (Manam & Ashfaq, 2022; Aminul & Shamima, 2022). These mechanisms can significantly strengthen privacy protections within financial ERP ecosystems by minimizing opportunities for unauthorized data exposure. The increasing sophistication of ransomware campaigns targeting public institutions has further elevated interest in Zero-Trust strategies because segmented networks and least-privilege controls may reduce the scale of operational disruption following cyber compromise. Public-sector cybersecurity modernization programs increasingly integrate Zero-Trust principles into broader digital governance initiatives involving cloud migration, identity management reform, and cybersecurity resilience planning (Lois et al., 2020; Shamsul & Sultan, 2022; Binte & Iftekhar, 2022). Quantitative assessment of these initiatives enables systematic analysis of whether Zero-Trust adoption produces statistically significant improvements in financial data privacy performance, cybersecurity governance efficiency, and ERP security effectiveness across public-sector institutions.

Public-sector ERP environments differ substantially from private-sector systems because governmental institutions operate under unique administrative, legal, and societal responsibilities involving transparency, accountability, and public service continuity. Financial management systems within public administration frequently support national budgeting operations, welfare distribution programs, infrastructure financing projects, healthcare expenditures, educational allocations, and procurement management processes. These functions involve extensive interdepartmental coordination and often require data sharing across multiple governmental entities (Bonsón & Bednárová, 2019). The complexity of these operational environments increases exposure to cybersecurity vulnerabilities associated with inconsistent access governance, fragmented legacy infrastructure, and inadequate identity management controls. Public institutions commonly maintain large-scale ERP ecosystems developed over extended periods through incremental technological expansion and policy adaptation. Such environments may contain outdated applications, incompatible software components, and decentralized authentication structures that complicate cybersecurity enforcement. Financial data privacy within these systems becomes particularly difficult to maintain because sensitive records are frequently accessed by diverse categories of users operating under varying authorization requirements. Zero-Trust Architecture offers a structured framework for addressing these challenges through centralized identity verification, contextual authentication, adaptive access control, and continuous monitoring practices (Abidin et al., 2019). The architecture promotes granular visibility into user behavior and access activity, thereby strengthening institutional capability to detect anomalies and unauthorized interactions involving financial information. International cybersecurity frameworks increasingly encourage public-sector institutions to adopt security models emphasizing identity-centric governance and continuous risk evaluation. The transition toward digital government services has amplified these priorities because online citizen portals, electronic payment systems, and cloud-hosted ERP applications expand the attack surface available to malicious actors. Public trust in governmental institutions is strongly connected to perceptions regarding the protection of sensitive financial and administrative information. Security failures involving public financial databases can therefore generate consequences extending beyond technical disruption into political credibility, economic confidence, and administrative legitimacy. Quantitative research examining Zero-Trust adoption within public-sector ERP systems contributes valuable empirical evidence regarding the relationship between cybersecurity architecture and

financial data privacy outcomes (Inuwa et al., 2020). Such analysis supports systematic evaluation of whether advanced authentication controls, segmented access models, and continuous verification mechanisms strengthen protection against unauthorized financial data exposure within complex governmental digital infrastructures.

The operationalization of Zero-Trust principles within ERP environments requires integration of multiple technological and organizational components that collectively influence financial data privacy outcomes. Identity and access management systems constitute foundational elements of Zero-Trust implementation because they regulate authentication procedures, user authorization levels, session monitoring, and privilege allocation practices (Olson & Wu, 2020). Multi-factor authentication mechanisms strengthen verification processes by requiring multiple forms of user validation before granting access to financial records or administrative functions. Behavioral analytics technologies further enhance security by identifying unusual user activity patterns that may indicate credential compromise or malicious intent. Network micro-segmentation strategies isolate critical financial databases and restrict lateral movement between ERP modules, thereby limiting exposure following unauthorized entry attempts. Encryption protocols protect data confidentiality during storage and transmission, reducing opportunities for interception or manipulation. Continuous monitoring platforms generate real-time visibility into access events, policy violations, and anomalous behaviors associated with financial information systems. These operational components collectively form a dynamic cybersecurity ecosystem designed to minimize implicit trust and maximize contextual verification. Public-sector institutions implementing Zero-Trust frameworks may experience measurable changes in privacy performance indicators such as reduced data breach frequency, improved compliance audit outcomes, enhanced incident detection rates, and lower unauthorized access occurrences (Kotka & Liiv, 2015; Taufiqur & Albert, 2022; Taufiqur & Khalid, 2022). Quantitative analysis becomes particularly important in evaluating these relationships because cybersecurity effectiveness often involves complex interactions between technological controls, user behavior, organizational governance, and operational processes. Statistical investigation can therefore provide objective evidence regarding the extent to which Zero-Trust adoption influences financial data privacy performance within governmental ERP systems. Such evidence is increasingly necessary because public institutions frequently allocate substantial financial resources toward cybersecurity modernization initiatives requiring accountability and measurable justification. The strategic importance of ERP cybersecurity has intensified as governments expand digital transformation programs involving cloud integration, electronic financial management systems, and cross-agency interoperability frameworks. These developments create operational opportunities while simultaneously increasing cybersecurity complexity (Litvinenko, 2020). Empirical examination of Zero-Trust implementation within public-sector financial environments consequently represents a critical area of investigation for understanding how contemporary cybersecurity architectures influence privacy protection, institutional resilience, and secure digital governance operations.

Quantitative research concerning Zero-Trust Architecture adoption within public-sector ERP environments holds substantial relevance for cybersecurity governance, digital transformation management, and financial information protection. The increasing convergence of cloud computing, artificial intelligence, remote access technologies, and interconnected digital services has transformed governmental ERP systems into highly dynamic infrastructures requiring adaptive security models. Public institutions now operate within cyber threat environments characterized by rapidly evolving attack methodologies targeting sensitive financial assets and administrative operations (Lee & Park, 2015). Traditional security approaches focused on static perimeter defenses have demonstrated limitations in addressing credential compromise, insider threats, unauthorized privilege escalation, and distributed access vulnerabilities. Zero-Trust Architecture introduces an alternative framework emphasizing continuous verification, contextual authentication, least-privilege principles, and granular access governance. Understanding the measurable impact of these practices on financial data privacy outcomes has become increasingly important for policymakers, cybersecurity administrators, ERP managers, and governmental technology strategists. Quantitative investigation enables structured evaluation of statistical relationships between Zero-Trust implementation variables and privacy performance indicators within public-sector ERP ecosystems (Nicho et al., 2017). Such indicators may

include breach reduction frequency, authentication effectiveness, compliance consistency, access control efficiency, and user accountability measures. Public-sector institutions face growing pressure to demonstrate effective stewardship of financial information resources because cybersecurity incidents involving governmental financial systems can undermine public trust, disrupt administrative operations, and generate substantial economic consequences. International digital governance initiatives increasingly emphasize secure information management, cyber resilience, and privacy-centered infrastructure development as foundational components of modern public administration. ERP systems remain central to these objectives because they integrate critical financial operations supporting governmental continuity and economic administration. The complexity of these systems requires cybersecurity frameworks capable of addressing both technological and human vulnerabilities within interconnected institutional environments (Joo & Hovav, 2016). Zero-Trust adoption consequently represents a significant area of inquiry within contemporary cybersecurity research. Quantitative examination of its relationship with financial data privacy in public-sector ERP environments contributes to expanding scholarly understanding regarding how identity-centric security architectures influence confidentiality protection, operational governance, and cybersecurity effectiveness within digitally transformed governmental institutions.

The primary objective of this quantitative study is to examine the relationship between Zero-Trust Architecture adoption and financial data privacy within public-sector Enterprise Resource Planning environments. The study seeks to evaluate how identity-centric cybersecurity frameworks influence the protection of sensitive financial information managed through governmental ERP systems. Public-sector institutions increasingly depend on integrated ERP infrastructures to support budgeting operations, payroll management, procurement activities, taxation systems, pension administration, and interdepartmental financial coordination. The growing complexity of these digital ecosystems has intensified concerns regarding unauthorized access, insider threats, data leakage, privilege misuse, and cyberattacks targeting confidential financial records. The study therefore aims to quantitatively assess whether the implementation of Zero-Trust principles contributes to measurable improvements in financial data privacy protection across public-sector digital infrastructures. The research specifically focuses on evaluating the effectiveness of continuous authentication mechanisms, least-privilege access controls, network segmentation strategies, behavioral monitoring systems, and identity verification protocols in reducing vulnerabilities associated with financial information exposure. Another objective of the study is to investigate the extent to which Zero-Trust adoption strengthens cybersecurity governance within ERP environments by enhancing access accountability, improving user authorization management, and minimizing opportunities for unauthorized lateral movement across interconnected governmental databases. The research also seeks to measure the influence of Zero-Trust implementation on organizational security performance indicators such as breach prevention capability, incident detection efficiency, access control reliability, and compliance management effectiveness. In addition, the study intends to examine whether public-sector institutions with higher levels of Zero-Trust integration demonstrate stronger financial data privacy outcomes compared to institutions operating under traditional perimeter-based security models. The quantitative approach supports statistical examination of relationships between cybersecurity architecture variables and financial privacy indicators, thereby generating objective evidence regarding the operational value of Zero-Trust frameworks within governmental ERP ecosystems. The study further aims to contribute empirical understanding regarding how modern cybersecurity models can support secure digital governance, institutional accountability, and financial information protection within increasingly interconnected public-sector technological environments characterized by expanding digital transformation initiatives and evolving cyber threat landscapes.

**LITERATURE REVIEW**

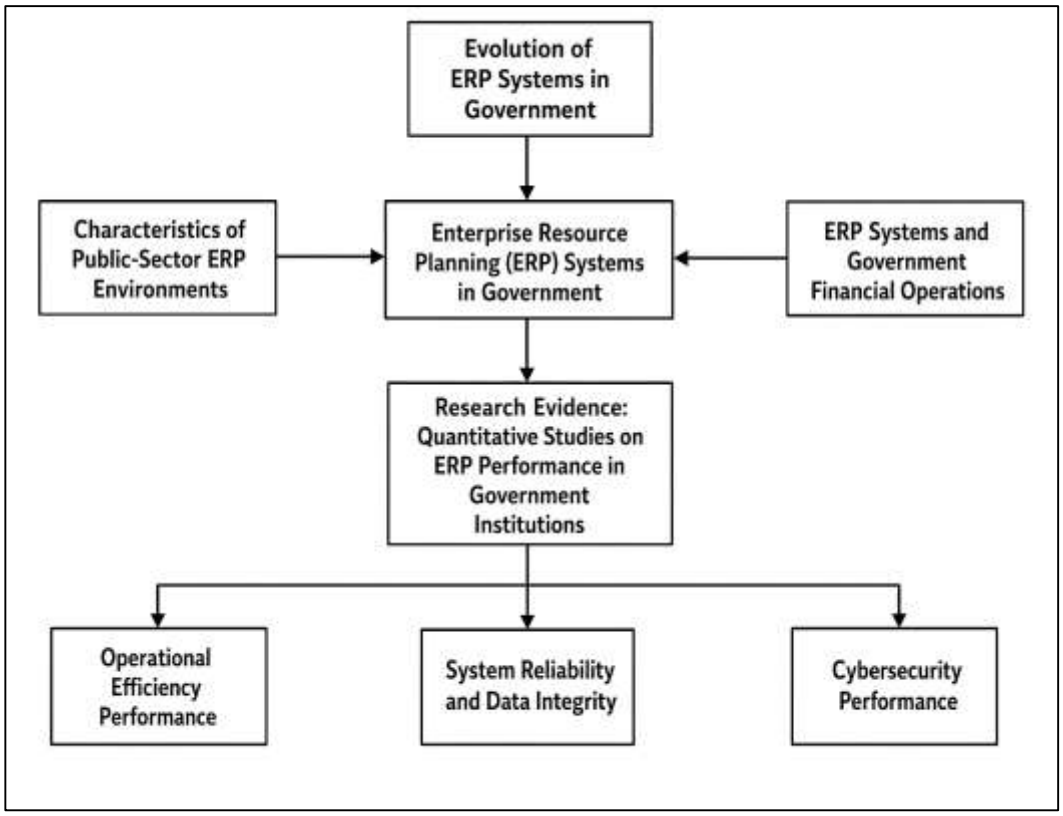
The literature review for this quantitative study examines the scholarly foundations, theoretical developments, empirical findings, and technological dimensions associated with Zero-Trust Architecture adoption and financial data privacy within public-sector Enterprise Resource Planning environments. The increasing digitalization of governmental financial operations has transformed ERP systems into highly interconnected infrastructures responsible for managing budgeting processes, procurement transactions, taxation records, payroll systems, pension administration, and interagency

financial communication. These systems contain extensive volumes of confidential financial information that require advanced cybersecurity protections capable of addressing sophisticated cyber threats, unauthorized access risks, insider vulnerabilities, and data governance challenges (Alsafi & Fan, 2020). The emergence of Zero-Trust Architecture as an identity-centric cybersecurity framework has generated substantial academic and institutional attention because of its emphasis on continuous authentication, least-privilege access, contextual verification, network segmentation, and persistent monitoring mechanisms. Existing literature demonstrates growing concern regarding the limitations of traditional perimeter-based cybersecurity models within complex public-sector digital ecosystems characterized by cloud integration, remote access environments, mobile technologies, and interconnected governmental databases. The literature review therefore synthesizes quantitative and empirical studies related to cybersecurity governance, ERP security frameworks, financial data privacy protection, identity and access management systems, insider threat mitigation, and Zero-Trust implementation effectiveness in organizational environments (Jaoude & Saade, 2019). The section further evaluates theoretical perspectives supporting cybersecurity modernization within public administration and examines measurable relationships between Zero-Trust controls and privacy performance indicators such as breach prevention capability, access control reliability, incident detection efficiency, compliance performance, and user accountability. In addition, the review explores the operational characteristics of public-sector ERP systems, the evolution of digital governance infrastructures, and the cybersecurity challenges associated with financial information management within governmental institutions. The literature also investigates technological variables influencing Zero-Trust adoption, including multi-factor authentication, behavioral analytics, encryption protocols, endpoint security mechanisms, and network micro-segmentation strategies. Quantitative studies examining cybersecurity effectiveness, privacy governance, institutional resilience, and ERP protection mechanisms are critically synthesized to establish a comprehensive scholarly foundation for the present study (Amadi-Echendu & Amadi-Echendu, 2016). Through systematic examination of existing research, the literature review identifies major conceptual relationships, methodological approaches, empirical gaps, and statistical patterns relevant to understanding how Zero-Trust Architecture adoption influences financial data privacy outcomes in public-sector ERP environments.

**Definition and Evolution of ERP Systems**

Enterprise Resource Planning systems are integrated technological infrastructures developed to centralize organizational processes, facilitate data sharing, and improve operational coordination across institutional departments. The historical evolution of ERP systems originated from material requirements planning and manufacturing resource planning technologies that emerged within industrial production sectors during the late twentieth century (Inkinen et al., 2019). Early ERP systems primarily focused on inventory management, manufacturing scheduling, logistics coordination, and accounting functions within private-sector organizations. Continuous technological advancement expanded ERP capabilities into broader organizational domains, including procurement, human resource administration, customer management, and financial reporting processes. The expansion of globalization, digital communication technologies, and internet-based infrastructures accelerated ERP adoption across multinational corporations seeking standardized operational frameworks and integrated decision-making systems. Public-sector institutions gradually recognized the administrative value of ERP technologies as governments pursued modernization initiatives aimed at improving efficiency, transparency, accountability, and service delivery (Zhang et al., 2020). The transition from private-sector ERP implementation to governmental adoption involved significant structural adaptation because public institutions operate within highly regulated administrative environments characterized by complex governance procedures, interdepartmental coordination requirements, and public accountability obligations. Governments increasingly integrated ERP systems into financial administration, taxation management, procurement operations, welfare distribution, and payroll processing infrastructures to support digital transformation strategies. Digital transformation within public administration created demand for centralized technological systems capable of managing large volumes of financial and administrative data across multiple governmental entities. ERP technologies therefore became foundational components of electronic governance initiatives designed to strengthen institutional efficiency and improve administrative coordination (Yoon, 2020).

**Figure 3: Evolution of ERP systems in government**




Functional integration across finance, procurement, human resources, and taxation modules enabled governments to standardize reporting procedures, automate transactional operations, and enhance data accessibility within centralized environments. Scholarly literature examining ERP evolution has emphasized the growing complexity of governmental information systems and the increasing importance of integrated digital infrastructures in supporting administrative modernization, financial governance, operational coordination, and organizational performance across public institutions (Gutwirth et al., 2015).

Public-sector ERP environments possess distinct operational characteristics shaped by governmental administrative structures, regulatory obligations, public accountability requirements, and large-scale institutional coordination processes. Centralized financial management systems constitute one of the defining features of governmental ERP infrastructures because public institutions require integrated platforms capable of coordinating budgeting, expenditure monitoring, procurement activities, payroll administration, and taxation management across multiple agencies and departments. Unlike private-sector organizations focused primarily on profitability and market performance, public-sector institutions operate within service-oriented frameworks emphasizing accountability, transparency, regulatory compliance, and efficient resource allocation (Bernroider et al., 2016). ERP systems in governmental settings therefore support broader administrative functions involving policy implementation, citizen service delivery, interdepartmental coordination, and public financial governance. Interagency operational integration represents another significant characteristic of public-sector ERP environments because governmental organizations frequently require continuous communication and data exchange between ministries, departments, municipalities, treasury offices, and regulatory authorities. These interconnected operational structures increase dependence on centralized databases and integrated technological infrastructures capable of supporting coordinated decision-making and standardized administrative procedures. Governmental data governance structures further distinguish public-sector ERP systems because public institutions must comply with legal standards related to financial reporting, information confidentiality, audit accountability, and records management (Gkika et al., 2020). Administrative policies governing access control, information

retention, authorization management, and data classification significantly influence ERP operational frameworks within governmental environments. The complexity of public financial information systems also contributes to the distinctive nature of public-sector ERP infrastructures. Governmental ERP systems often process extensive volumes of sensitive financial data involving taxation records, procurement transactions, pension information, welfare allocations, and national budget management activities. This operational complexity increases technological dependency while simultaneously creating cybersecurity and governance challenges related to data integrity, access control, privacy protection, and operational reliability (Al-Ruithe et al., 2019). Existing literature highlights that public-sector ERP environments require highly coordinated technological governance structures capable of balancing administrative efficiency, financial accountability, institutional transparency, and information security within digitally integrated governmental ecosystems.

ERP systems play a critical role in supporting government financial operations through the automation, coordination, and integration of essential administrative processes associated with public resource management. Budget management automation represents one of the most significant functions of governmental ERP systems because public institutions require continuous monitoring of expenditures, revenue allocation, budget forecasting, and financial reporting activities across multiple administrative units (Skafi et al., 2020). ERP technologies enable centralized budgeting platforms that support real-time financial analysis, expenditure tracking, and regulatory compliance monitoring within governmental financial systems. Public procurement systems also rely extensively on ERP infrastructures to coordinate supplier management, tender administration, contract processing, purchasing activities, and expenditure authorization procedures. Procurement integration within ERP environments improves administrative transparency, standardizes procurement workflows, and enhances accountability in public financial transactions. Tax administration infrastructures constitute another essential component of governmental ERP operations because taxation systems require efficient data processing capabilities capable of managing revenue collection, taxpayer records, audit documentation, compliance reporting, and interagency information sharing (Falagara Sigala et al., 2020). ERP systems support tax administration by facilitating centralized data management, automated transaction processing, and coordinated financial analysis across taxation authorities and treasury institutions. Payroll and pension management systems similarly depend on ERP technologies to administer salary processing, employee benefits, retirement contributions, pension distribution, and workforce financial records within public administration. The integration of payroll and pension functions into ERP environments improves operational consistency and reduces administrative inefficiencies associated with manual processing procedures (Al Barghuthi et al., 2019). Scholarly literature examining ERP systems within government financial operations has emphasized the relationship between technological integration and administrative efficiency, highlighting how centralized ERP infrastructures contribute to improved financial coordination, enhanced reporting accuracy, standardized operational procedures, and strengthened public accountability. Research also demonstrates that ERP implementation within governmental financial systems supports organizational transparency by enabling real-time access to financial information, automated audit trails, and integrated performance monitoring capabilities across interconnected public institutions (Almond & van Erp, 2020).

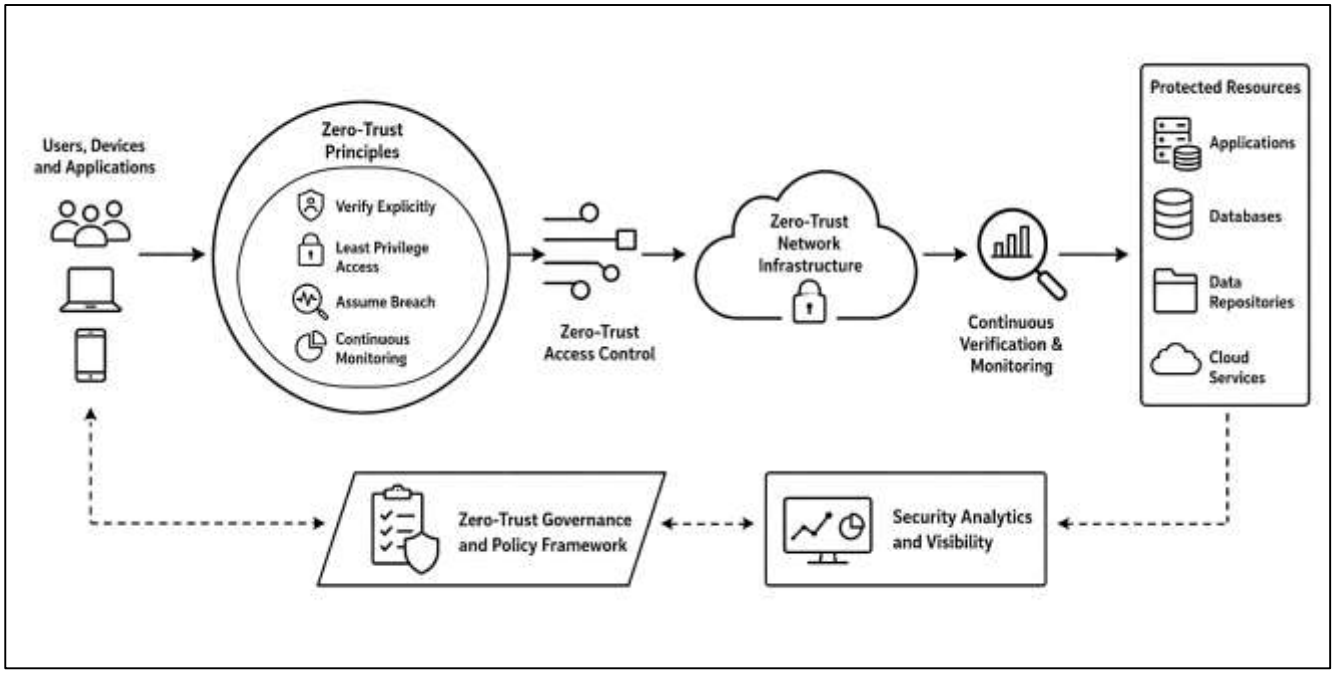
Quantitative studies examining ERP performance in government institutions have increasingly focused on operational efficiency, adoption effectiveness, system reliability, and cybersecurity performance within public-sector digital environments. ERP operational efficiency metrics commonly evaluate improvements in transaction processing speed, administrative coordination, data accessibility, workflow automation, financial reporting accuracy, and resource utilization following ERP implementation. Empirical studies have identified significant relationships between ERP integration and enhanced governmental operational performance, particularly in areas involving procurement management, payroll administration, budgeting processes, and financial coordination (Althonayan & Althonayan, 2017). ERP adoption success indicators frequently include user acceptance levels, implementation completion rates, institutional integration effectiveness, organizational readiness, and employee adaptation to digital administrative systems. Quantitative analyses examining governmental ERP adoption have emphasized the importance of technological infrastructure quality, administrative

leadership support, employee training, and institutional governance frameworks in determining implementation success. Statistical analysis of ERP system reliability has also become a significant area of scholarly investigation because public institutions depend heavily on continuous system availability, accurate data processing, and operational consistency within financial management environments. Researchers have measured system reliability through indicators such as downtime frequency, processing error rates, transaction accuracy, database consistency, and infrastructure stability across governmental ERP platforms (Fernandez et al., 2017). Quantitative evaluation of ERP cybersecurity performance has gained increasing importance as public-sector institutions experience growing exposure to cyber threats targeting financial databases and administrative systems. Empirical studies examining ERP cybersecurity commonly analyze access control effectiveness, incident response capability, authentication reliability, breach prevention efficiency, and organizational vulnerability management practices within governmental infrastructures. Research findings indicate that cybersecurity performance within ERP systems is strongly associated with institutional governance quality, technological integration maturity, employee security awareness, and implementation of advanced access management frameworks. Existing quantitative literature therefore demonstrates that ERP performance in government institutions extends beyond operational efficiency and includes broader dimensions related to administrative reliability, information security, financial governance, organizational resilience, and institutional accountability within increasingly digital public-sector environments (Shafi et al., 2019).

**Theoretical Foundations of Zero-Trust Architecture**

Zero-Trust Architecture represents a cybersecurity framework developed to address the growing complexity of digital infrastructures, interconnected organizational networks, and evolving cyber threats affecting modern institutions. The theoretical foundation of Zero-Trust Architecture is based on the principle that no user, device, application, or network component should receive automatic trust regardless of its location within or outside an organizational environment. Traditional cybersecurity models historically relied on perimeter-based protections that assumed internal networks were secure once access was granted through external defenses. Increasing digital transformation, cloud integration, remote access technologies, and mobile computing environments weakened the effectiveness of these assumptions and contributed to the emergence of identity-centric cybersecurity frameworks (Kharuddin et al., 2015). Zero-Trust Architecture therefore shifted cybersecurity focus from network location to continuous identity verification and contextual authentication processes. Identity-centric cybersecurity frameworks emphasize strict validation of users, devices, and applications before permitting access to organizational resources, particularly sensitive financial and administrative information. Continuous authentication principles further strengthen this framework by requiring persistent monitoring and verification throughout user sessions rather than relying solely on initial login authentication. The concept of least-privilege access governance also constitutes a central component of Zero-Trust theory because users are granted only the minimum level of system access necessary to perform authorized responsibilities. This approach reduces opportunities for unauthorized lateral movement, privilege escalation, and internal misuse within complex organizational systems. Network segmentation and access verification mechanisms complement these principles by dividing digital infrastructures into isolated security zones that limit unrestricted movement across organizational databases and applications (Chaushi et al., 2018). Existing literature examining Zero-Trust Architecture highlights its importance in strengthening cybersecurity resilience within governmental and enterprise environments characterized by expanding digital dependency and increasing exposure to sophisticated cyber threats. Scholarly studies further emphasize that Zero-Trust principles support stronger information governance, improved access accountability, enhanced identity management, and more effective protection of sensitive institutional data within highly interconnected technological ecosystems (Lutfi, 2020).

**Figure 4: Zero-trust architecture flowchart diagram**



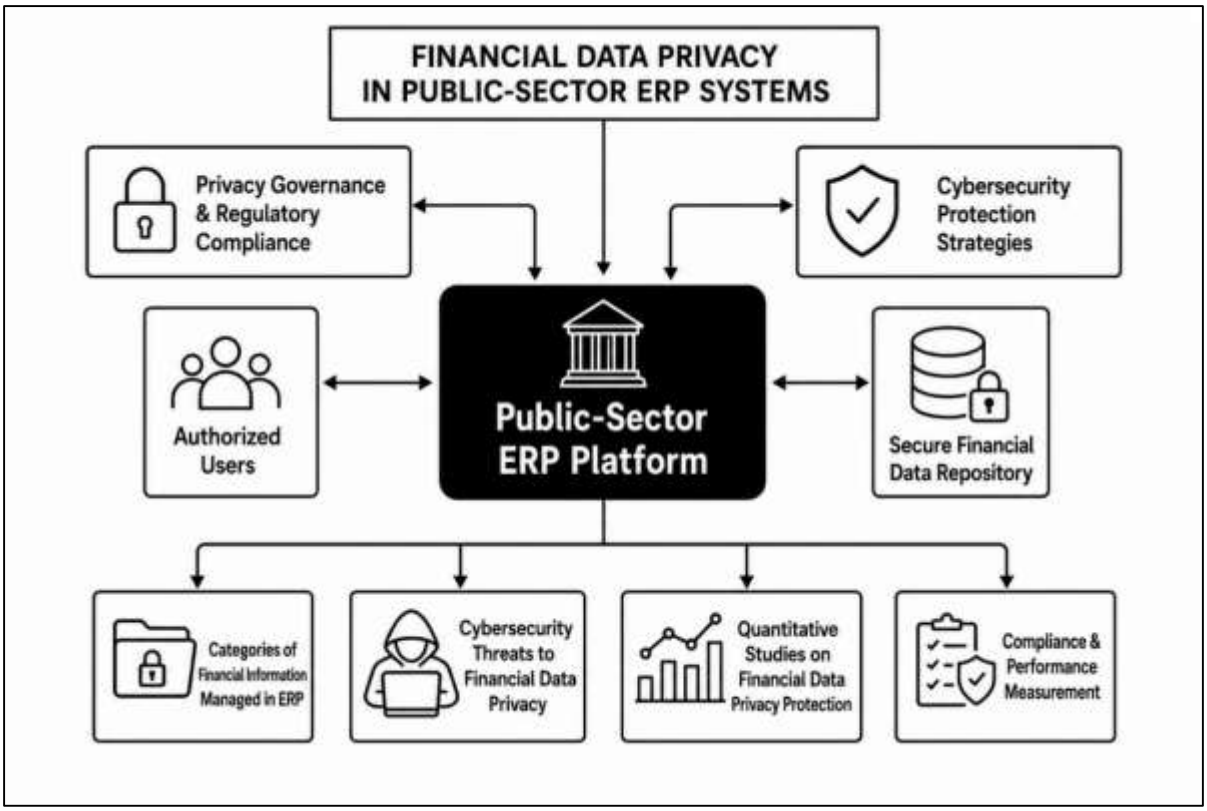

The evolution from traditional perimeter-based cybersecurity frameworks to Zero-Trust security models emerged from growing recognition that conventional network defenses were insufficient for addressing modern cyber threats within digitally interconnected environments. Traditional cybersecurity strategies were primarily designed around the assumption that organizational networks could be protected through external barriers such as firewalls, intrusion prevention systems, and gateway security controls. Once users or devices gained entry into internal networks, they frequently received broad access privileges with limited ongoing verification or behavioral monitoring. The expansion of cloud computing, remote workforce technologies, mobile applications, and internet-connected devices significantly altered organizational operating environments and exposed limitations within perimeter-based security architectures (Gupta et al., 2018). Cybersecurity incidents increasingly originated from compromised internal accounts, malicious insiders, phishing attacks, credential theft, and unauthorized privilege escalation activities that bypassed traditional defensive boundaries. Governmental systems became particularly vulnerable because public-sector institutions often operate large-scale interconnected infrastructures involving multiple agencies, departments, and external service providers. Internal threat exposure within governmental systems therefore became a major concern in cybersecurity literature, particularly in relation to financial management systems, taxation databases, procurement platforms, and citizen information repositories. Cloud-based security transformation further accelerated the movement toward Zero-Trust models because cloud environments eliminated clearly defined network perimeters and increased dependence on distributed access infrastructures (Peters & Aggrey, 2019). Organizations increasingly required adaptive security strategies capable of authenticating users and validating devices regardless of physical network location. Cybersecurity modernization strategies consequently shifted toward identity-centric governance models emphasizing continuous verification, contextual authentication, restricted access privileges, and persistent activity monitoring. Existing scholarly research examining cybersecurity evolution has highlighted the importance of Zero-Trust adoption in strengthening organizational resilience against sophisticated attack methodologies targeting both external and internal vulnerabilities. Literature also demonstrates that Zero-Trust models support improved operational visibility, stronger governance structures, enhanced authentication management, and more effective containment of cybersecurity risks within highly integrated governmental and enterprise environments (Al Mahrami & Hakro, 2018).

The operational effectiveness of Zero-Trust Architecture is supported through several interconnected technological and governance components designed to strengthen cybersecurity protection within complex organizational infrastructures. Identity and access management systems represent one of the most critical components of Zero-Trust implementation because they regulate authentication procedures, authorization controls, user privileges, and access governance across digital environments. These systems establish centralized mechanisms for verifying user identities and managing permissions associated with organizational resources, particularly sensitive financial and administrative information (Poba-Nzaou et al., 2014). Multi-factor authentication technologies further strengthen security by requiring users to provide multiple forms of verification before accessing protected systems or databases. This layered authentication approach reduces the risk associated with compromised passwords and unauthorized account access within interconnected technological environments. Behavioral analytics and monitoring systems also play a significant role in Zero-Trust Architecture by continuously evaluating user activities, access patterns, device behavior, and transactional anomalies to identify potential cybersecurity threats. These monitoring mechanisms enhance institutional visibility into network activities and improve the ability to detect suspicious behavior associated with credential misuse, insider threats, or unauthorized data access. Endpoint security validation mechanisms constitute another essential component because Zero-Trust frameworks require continuous assessment of devices attempting to connect to organizational systems (Abdellatif, 2014). Device validation processes evaluate security conditions such as software updates, malware exposure, compliance status, and configuration integrity before granting access permissions. Existing literature examining Zero-Trust operational structures emphasizes that cybersecurity effectiveness depends on the integration of these interconnected components within coordinated governance frameworks. Research findings indicate that organizations implementing strong identity governance systems, adaptive authentication technologies, real-time monitoring infrastructures, and endpoint validation protocols demonstrate improved resilience against cybersecurity incidents affecting sensitive institutional data. Scholarly discussions further highlight that Zero-Trust components collectively support stronger access accountability, improved information confidentiality, enhanced threat detection capabilities, and more effective governance of complex digital infrastructures operating within both public-sector and enterprise environments (Ahmad et al., 2015).

**Financial Data Privacy in Public-Sector ERP Systems**

Financial data privacy within public-sector ERP systems refers to the protection, confidentiality, controlled access, and ethical management of sensitive governmental financial information stored and processed within integrated digital infrastructures. Public-sector institutions manage extensive volumes of confidential data associated with taxation records, public expenditures, payroll systems, pension funds, procurement transactions, welfare distribution programs, and budget allocations. The increasing digitalization of government operations has significantly expanded dependence on ERP platforms for financial coordination and administrative management, thereby intensifying concerns regarding information confidentiality and unauthorized data exposure (Setyawan et al., 2020). Existing literature emphasizes that financial data privacy extends beyond technical security measures and incorporates broader governance dimensions involving accountability, transparency, ethical responsibility, and regulatory compliance within public administration. Governmental institutions are required to maintain strict protection standards because exposure of financial records may undermine public trust, compromise institutional credibility, and create opportunities for fraud, corruption, or unauthorized financial manipulation. Privacy governance in public institutions therefore involves coordinated administrative policies regulating data classification, access authorization, information retention, audit accountability, and user responsibility within centralized ERP environments (de Castro Silva & de Oliveira, 2015).

**Figure 5: Financial data privacy in public-sector ERP**




Regulatory requirements for financial data protection further strengthen institutional obligations by establishing legal frameworks governing confidentiality management, cybersecurity compliance, financial reporting standards, and information access restrictions. Ethical dimensions of public financial privacy also occupy a central position in scholarly discussions because governmental institutions possess responsibility for protecting citizen information while ensuring fair, transparent, and accountable management of public financial resources. Research literature consistently highlights that financial data privacy represents a multidimensional concept shaped by technological infrastructures, cybersecurity governance practices, legal compliance mechanisms, and institutional accountability structures (Galy & Sauceda, 2014). Public-sector ERP systems therefore require highly coordinated privacy management frameworks capable of balancing operational efficiency, administrative transparency, financial accountability, and secure information protection within increasingly interconnected governmental environments characterized by growing digital dependency and expanding cybersecurity risks.

Public-sector ERP systems manage diverse categories of financial information that support governmental administration, public resource allocation, and institutional financial coordination across interconnected agencies and departments. Taxpayer financial records represent one of the most sensitive categories of information processed within governmental ERP environments because tax administration systems contain confidential data involving income declarations, revenue collection, payment histories, compliance records, banking details, and audit documentation (Trigo et al., 2014). The protection of taxpayer information is considered essential for maintaining public trust, institutional credibility, and regulatory compliance within digital governance systems. Government payroll databases also constitute critical ERP components because they store extensive employee financial information, including salary structures, tax deductions, pension contributions, healthcare benefits, employment classifications, and banking details associated with public-sector personnel. ERP integration enables centralized payroll processing and administrative coordination while simultaneously increasing the importance of strict confidentiality controls and access governance mechanisms. Procurement and expenditure information represent another significant category of financial data managed within public-sector ERP systems. Government procurement infrastructures

process contracts, supplier records, purchasing activities, expenditure approvals, tender documentation, and budget allocations associated with public service delivery and infrastructure development (Ali & Miller, 2017). Existing literature identifies procurement systems as particularly vulnerable to financial fraud, unauthorized transactions, and corruption-related risks when cybersecurity protections are insufficient. Pension and welfare distribution records also require extensive protection because these systems contain sensitive financial information associated with retirement benefits, social assistance programs, healthcare subsidies, and public welfare payments involving large populations of citizens. Scholarly research examining ERP financial information management highlights the increasing complexity of public-sector databases and the growing dependence on centralized technological systems capable of coordinating sensitive administrative operations. Literature further demonstrates that effective financial information protection requires strong governance structures, secure access management systems, continuous monitoring mechanisms, and institutional accountability frameworks designed to safeguard confidential public financial records within integrated governmental ERP environments (Hiebl et al., 2017).

Cybersecurity threats targeting financial data privacy within public-sector ERP systems have increased significantly alongside the expansion of digital governance infrastructures and interconnected administrative technologies. Unauthorized access incidents represent one of the most common threats identified in existing literature because attackers frequently exploit weak authentication controls, compromised credentials, misconfigured access permissions, and vulnerable network infrastructures to gain entry into governmental financial systems. Public-sector ERP environments are particularly attractive targets due to the high strategic and economic value of the sensitive financial information they contain. Insider threat vulnerabilities also constitute a major concern within governmental institutions because employees, contractors, or administrative personnel with authorized system access may intentionally or unintentionally expose confidential financial records (de Azevedo et al., 2020). Scholarly studies examining insider threats highlight the importance of access governance, user accountability, behavioral monitoring, and privilege management in reducing internal cybersecurity risks affecting public financial databases. Credential theft and phishing attacks have similarly emerged as major cybersecurity challenges within governmental ERP systems because attackers increasingly rely on social engineering techniques to obtain unauthorized access to financial information infrastructures. Phishing campaigns targeting public-sector employees frequently exploit human vulnerabilities through deceptive communications designed to compromise login credentials, financial authorization systems, or administrative access privileges. Financial ransomware attacks targeting governments have also become a growing area of concern in cybersecurity literature because ransomware incidents can disrupt essential public services, compromise financial operations, and expose confidential institutional data (Chang et al., 2014). ERP systems supporting taxation, budgeting, payroll, procurement, and welfare administration are often central targets due to their operational importance and extensive data repositories. Existing scholarly research consistently demonstrates that cybersecurity threats affecting financial data privacy involve both technological vulnerabilities and organizational governance weaknesses within public-sector institutions. Literature further emphasizes that effective protection of governmental financial information requires coordinated cybersecurity strategies integrating authentication controls, monitoring technologies, user awareness programs, incident response mechanisms, and institutional governance frameworks capable of addressing complex and evolving cyber threats within centralized ERP environments (Jagoda & Samaranayake, 2017).

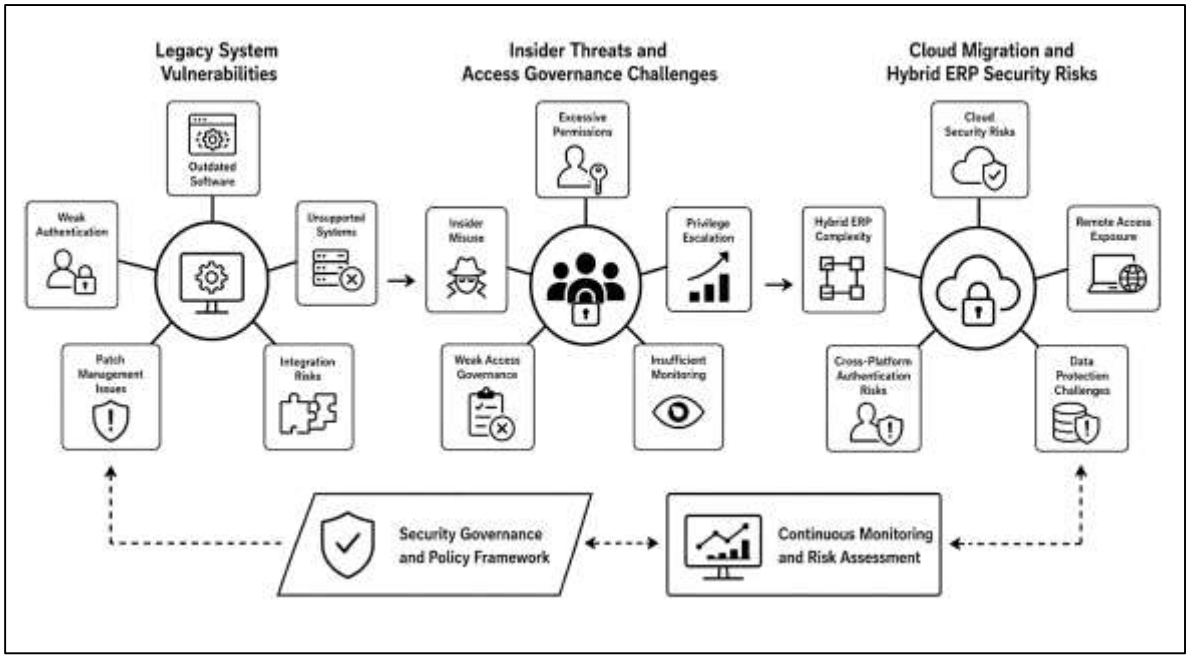
Quantitative studies examining financial data privacy protection within public-sector ERP systems have focused extensively on measuring cybersecurity effectiveness, breach prevention capability, data exposure risks, and compliance performance across governmental digital infrastructures. Statistical analysis of privacy breach frequency represents a significant area of empirical research because public institutions increasingly require measurable evidence regarding the effectiveness of cybersecurity controls in protecting confidential financial information. Existing studies commonly evaluate breach incidents through indicators such as unauthorized access occurrences, financial data exposure events, credential compromise frequency, and system intrusion rates within governmental ERP environments (Huang & Handfield, 2015). Quantitative assessment of data leakage risks has also received substantial

scholarly attention because centralized ERP systems process extensive volumes of sensitive financial information vulnerable to accidental disclosure, insider misuse, and external cyberattacks. Researchers frequently examine relationships between access governance mechanisms, authentication systems, employee security practices, and organizational vulnerability exposure in evaluating financial privacy protection effectiveness. Financial information exposure measurements further contribute to quantitative cybersecurity literature by assessing the extent of confidential data compromise during security incidents involving public-sector financial systems. Studies evaluating exposure severity often consider variables such as the number of affected records, duration of unauthorized access, financial transaction disruption, and organizational recovery performance following cybersecurity breaches (Hustad et al., 2016). Privacy compliance performance indicators similarly constitute an important area of quantitative investigation because governmental institutions operate under strict regulatory obligations involving financial confidentiality, audit accountability, and information protection standards. Empirical research commonly measures compliance performance through audit outcomes, policy adherence rates, regulatory violation frequency, and implementation effectiveness of cybersecurity governance frameworks within ERP environments. Existing literature consistently demonstrates that financial data privacy protection is strongly associated with organizational governance quality, cybersecurity infrastructure maturity, authentication reliability, and institutional commitment to secure information management practices (Appelbaum et al., 2017). Quantitative findings also indicate that public-sector institutions implementing advanced access management systems, continuous monitoring technologies, and coordinated privacy governance structures frequently demonstrate stronger financial data protection performance within increasingly digital administrative environments.

**Cybersecurity Challenges in Public-Sector ERP Environments**

Legacy system vulnerabilities represent a major cybersecurity challenge in public-sector ERP environments because many governmental institutions continue to operate outdated software infrastructures that were developed before current cybersecurity risks, cloud integration models, and identity-based access controls became central to digital governance. Public agencies often depend on long-standing ERP platforms that support budgeting, procurement, payroll, taxation, pension administration, and public expenditure management, making replacement or modernization difficult due to cost, operational disruption, regulatory dependency, and institutional complexity (Di Salvo, 2018). Literature on public-sector information systems indicates that legacy ERP platforms frequently contain outdated code structures, unsupported operating systems, weak authentication mechanisms, limited encryption capacity, and fragmented database connections. These weaknesses increase exposure to unauthorized access, malware intrusion, data leakage, and operational failure. Security limitations in legacy ERP platforms are also intensified by the presence of older modules that were designed for internal administrative use rather than highly connected digital ecosystems. As public-sector databases become more integrated across ministries, municipal authorities, treasury departments, and regulatory agencies, legacy systems may create integration risks because older applications often lack secure interoperability standards. Patch management deficiencies further contribute to ERP vulnerability because delayed updates, unsupported vendor systems, inconsistent maintenance schedules, and limited cybersecurity staffing can leave known weaknesses unresolved (Elbahri et al., 2019). Quantitative cybersecurity studies commonly identify patch delays, system age, configuration gaps, and outdated authentication models as measurable contributors to breach probability and system reliability problems. Therefore, legacy ERP vulnerability is not only a technical issue but also an institutional governance concern involving resource allocation, modernization planning, administrative continuity, and financial data protection.

**Figure 6: Legacy system vulnerabilities and governance flowchart**




Insider threats and access governance challenges are significant concerns in public-sector ERP environments because governmental systems are used by large numbers of employees, administrators, contractors, auditors, vendors, and interagency personnel with different levels of authorization. Literature on ERP cybersecurity emphasizes that insider risks may occur through intentional misuse, accidental disclosure, weak password practices, excessive permissions, poor role separation, and limited monitoring of privileged activities (Wang & Wang, 2019). Employee access misuse is particularly serious in public financial systems because ERP platforms often contain sensitive records related to payroll, procurement, tax administration, pension payments, supplier contracts, and budget allocations. When users possess broader permissions than required for their job roles, public institutions become more vulnerable to unauthorized data viewing, financial manipulation, transaction abuse, and confidential record exposure. Privilege escalation vulnerabilities also create major risks because attackers or negligent insiders may exploit weak access controls to move from ordinary user accounts to higher-level administrative functions. Human factors remain central to ERP cybersecurity because staff behavior, training quality, awareness of phishing threats, compliance with access policies, and response to suspicious system activity all affect the strength of financial data protection. Access accountability failures are frequently discussed in cybersecurity literature as a major weakness when institutions lack clear audit trails, user activity logs, segregation of duties, and automated alerts for abnormal behavior (Núñez-Merino et al., 2020). Quantitative studies often measure insider risk through access violation frequency, unauthorized login attempts, privilege misuse incidents, policy noncompliance rates, and audit exception records. In public-sector ERP environments, strong access governance therefore requires structured identity management, role-based authorization, continuous monitoring, and institutional accountability mechanisms that reduce human-driven security weaknesses.

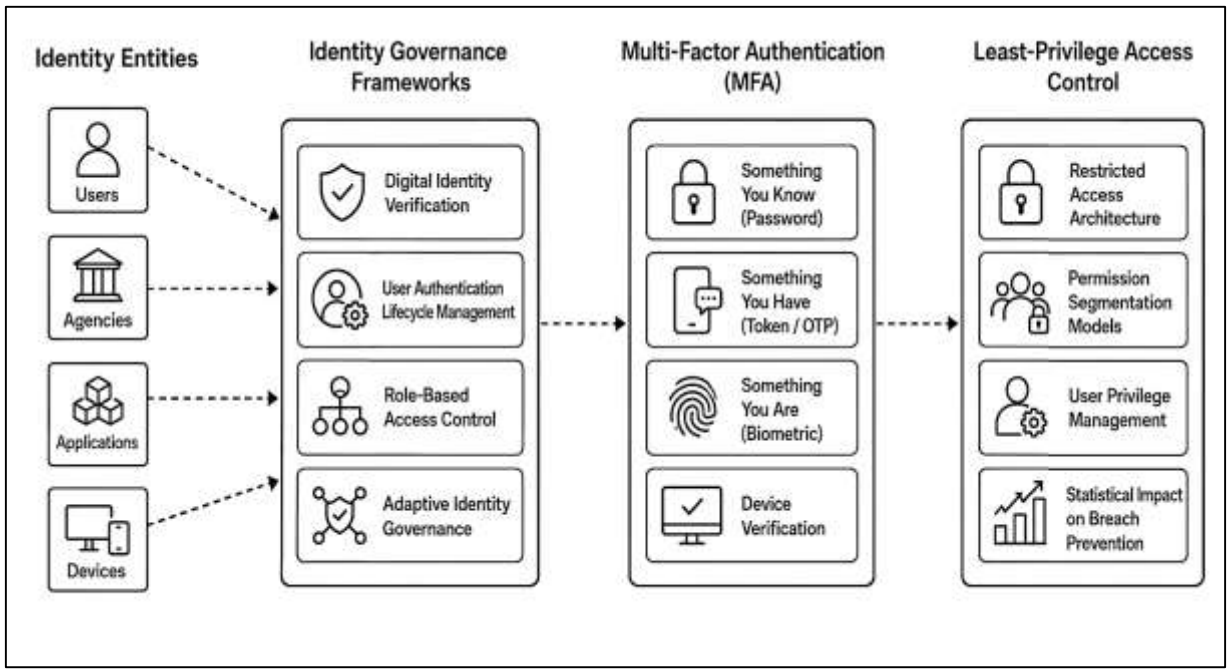
Cloud migration and hybrid ERP security risks have become increasingly important in public-sector cybersecurity literature as governmental institutions adopt cloud-based platforms, remote access systems, and distributed digital infrastructures to improve operational efficiency and service delivery (Lois et al., 2020). Cloud-based ERP implementation offers advantages such as scalability, centralized updates, data accessibility, and improved interagency coordination, but it also creates security challenges related to data residency, vendor dependency, shared responsibility models, configuration errors, and cross-platform access control. Public-sector institutions often operate hybrid ERP environments in which legacy on-premises systems are connected with cloud applications, third-party services, mobile access portals, and digital citizen-service platforms. This hybrid structure can increase

vulnerability because inconsistent security policies across platforms may create authentication gaps, data synchronization risks, and monitoring limitations. Remote access security exposure is another major concern because employees and contractors may connect to ERP systems from different devices, networks, and locations, increasing the possibility of credential theft, endpoint compromise, phishing attacks, and unauthorized system entry (Inkinen et al., 2019). Cross-platform authentication risks also arise when public institutions use multiple identity systems, outdated login protocols, or weak integration between cloud and internal ERP modules. Literature on cybersecurity modernization highlights that hybrid ERP security depends on strong identity and access management, encryption, endpoint validation, continuous monitoring, vendor risk assessment, and secure configuration practices. Quantitative research commonly evaluates cloud and hybrid ERP risk through breach frequency, misconfiguration rates, unauthorized access attempts, authentication failure patterns, downtime events, and incident response performance. In public-sector financial environments, cloud migration must therefore be understood as both a technological transformation and a cybersecurity governance challenge requiring careful protection of confidential financial information across interconnected digital platforms (Bernroider et al., 2016).

**Identity and Access Management in Zero-Trust ERP Security**

Identity governance frameworks represent a foundational component of Zero-Trust ERP security because they regulate how users, devices, applications, and administrative entities access sensitive organizational resources within interconnected digital infrastructures. Existing literature emphasizes that public-sector ERP systems process highly confidential financial and administrative information involving payroll management, taxation systems, procurement databases, pension records, and governmental budgeting operations, thereby requiring strong identity verification and access governance structures. Digital identity verification systems are designed to authenticate user identities before access is granted to institutional resources, ensuring that only authorized individuals interact with sensitive data environments (Liu et al., 2020). Scholarly studies indicate that identity verification mechanisms improve institutional accountability by reducing unauthorized access opportunities and strengthening visibility into user activities across ERP platforms. User authentication lifecycle management also constitutes a major area of discussion in cybersecurity literature because access governance extends beyond initial login verification and includes account provisioning, credential management, role modification, session monitoring, and account termination processes. Effective lifecycle management supports continuous security monitoring and reduces risks associated with dormant accounts, credential misuse, and unauthorized privilege retention within governmental systems. Role-based access control mechanisms further strengthen ERP security by assigning permissions according to organizational responsibilities rather than unrestricted system-wide access (Adu, 2018). Research examining public-sector cybersecurity consistently demonstrates that role-based access models reduce insider vulnerabilities and improve administrative accountability through structured authorization procedures. Adaptive identity governance structures additionally support cybersecurity resilience by dynamically adjusting access permissions based on contextual variables such as user behavior, location, device status, and operational risk conditions. Existing literature therefore identifies identity governance frameworks as critical institutional mechanisms supporting secure access management, operational transparency, cybersecurity accountability, and financial data protection within public-sector ERP environments characterized by increasing digital complexity and interconnected administrative infrastructures (Mohamed et al., 2019).

**Figure 7: Identity security architecture overview**




Multi-factor authentication has emerged as one of the most widely discussed security mechanisms within Zero-Trust ERP literature because of its effectiveness in strengthening identity verification and reducing unauthorized system access. Public-sector ERP systems frequently contain highly sensitive financial information associated with budgeting, procurement, payroll administration, tax records, and pension management, making authentication security a critical component of institutional cybersecurity governance. Existing research indicates that reliance on single-password authentication systems creates substantial vulnerabilities because attackers commonly exploit weak credentials, password reuse, phishing attacks, and credential theft techniques to gain unauthorized access to organizational networks (Nortje & Grobbelaar, 2020). Multi-factor authentication strengthens ERP security by requiring users to provide multiple forms of verification before access is granted, such as passwords, biometric identification, security tokens, or device-based confirmation mechanisms. Literature examining authentication reliability indicators consistently demonstrates that multi-factor authentication reduces account compromise risks and improves access accountability within complex digital environments. MFA implementation effectiveness has been evaluated across governmental and enterprise systems through measurements involving login accuracy, unauthorized access reduction, credential compromise prevention, and user authentication success rates. Quantitative studies commonly report measurable reductions in phishing-related breaches and credential-based intrusions following MFA adoption within financial and administrative infrastructures. Authentication success rate analysis also plays a significant role in cybersecurity evaluation because public institutions require authentication systems that maintain security while supporting operational efficiency and administrative continuity (Røberg et al., 2014). Existing literature highlights that poorly designed authentication procedures may reduce usability and increase employee resistance, while effective MFA systems balance accessibility with strong identity protection. Scholarly discussions further emphasize that multi-factor authentication contributes to broader Zero-Trust principles by reinforcing continuous verification, strengthening identity-centric security governance, and limiting unauthorized movement across interconnected ERP modules. As a result, MFA is widely recognized in cybersecurity literature as a critical security control supporting financial data confidentiality, institutional resilience, and secure access management within public-sector ERP environments (Das, 2019).

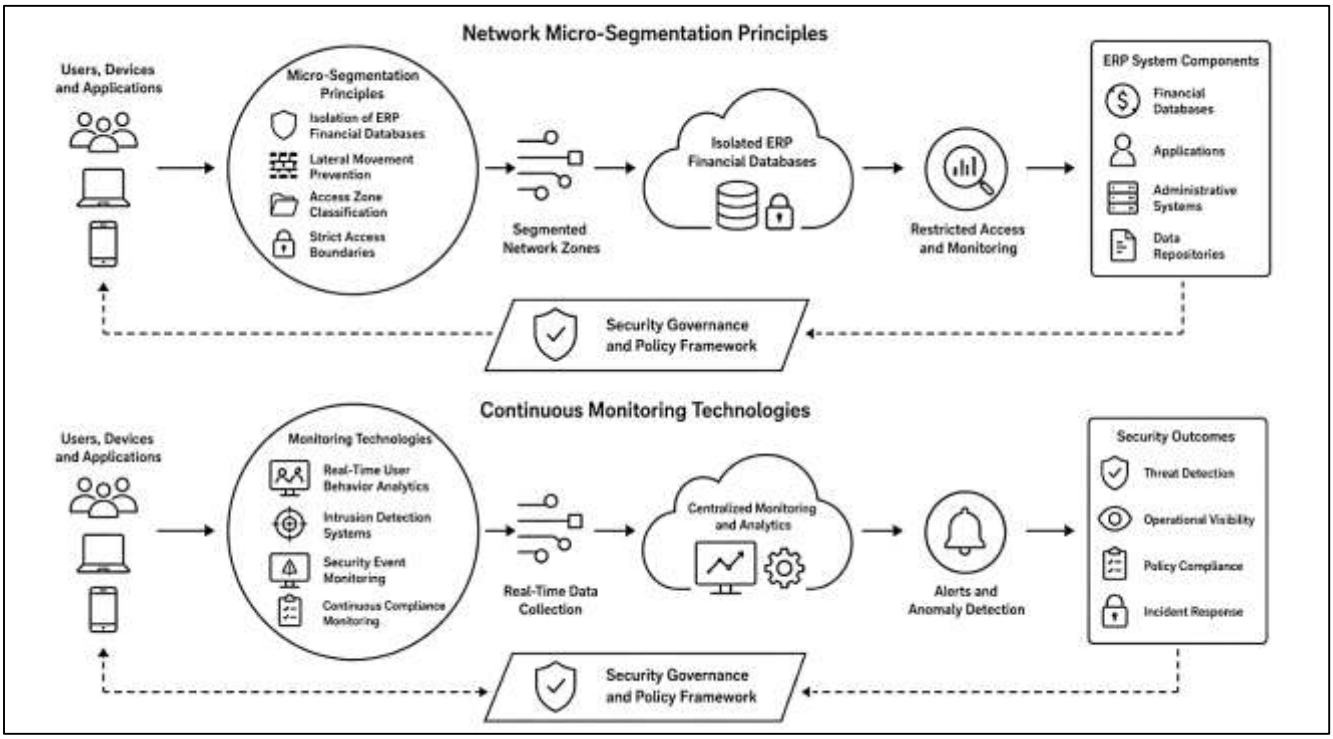
Least-privilege access control mechanisms constitute a central principle of Zero-Trust ERP security because they restrict users to the minimum level of access necessary to perform authorized organizational responsibilities. Existing literature consistently identifies excessive system privileges as a major contributor to cybersecurity incidents involving unauthorized access, insider misuse, data

leakage, and privilege escalation within public-sector ERP systems. Governmental ERP environments frequently involve interconnected modules supporting procurement operations, financial reporting, taxation management, payroll processing, and pension administration, making unrestricted access particularly dangerous for institutional security and financial data privacy. Restricted access architecture is therefore designed to minimize unnecessary user permissions and reduce opportunities for unauthorized interaction with confidential information (Abu-Shanab & Shehabat, 2018). Scholarly studies emphasize that access restrictions strengthen cybersecurity resilience by limiting lateral movement across organizational systems and reducing the impact of compromised user accounts. Permission segmentation models further support secure ERP governance by dividing access rights according to organizational roles, administrative functions, operational responsibilities, and security classifications. Literature examining permission segmentation demonstrates that structured access boundaries improve monitoring capability, accountability enforcement, and incident containment within interconnected digital environments. User privilege management systems also play a major role in cybersecurity governance because they regulate how permissions are assigned, modified, monitored, and revoked throughout the user lifecycle (Lee & Park, 2015). Existing research highlights that ineffective privilege management contributes significantly to internal vulnerabilities affecting public financial systems. Statistical impact on breach prevention has become an important area of quantitative cybersecurity investigation, with studies commonly measuring the relationship between restricted access policies and reductions in unauthorized transactions, financial data exposure, insider misuse incidents, and account compromise severity. Literature therefore demonstrates that least-privilege access mechanisms provide important security benefits by improving access accountability, reducing institutional vulnerability, strengthening financial data protection, and supporting operational control within public-sector ERP infrastructures operating under Zero-Trust security frameworks (Bonsón & Bednárová, 2019).

**Network Segmentation and Continuous Monitoring in Zero-Trust Architecture**

Network micro-segmentation principles represent a major component of Zero-Trust Architecture because they strengthen cybersecurity protection by dividing organizational networks into isolated security zones that restrict unauthorized movement across interconnected systems. Existing literature emphasizes that public-sector ERP environments frequently contain centralized financial databases managing taxation records, payroll systems, procurement transactions, pension information, and budget administration activities, making unrestricted network access highly dangerous for institutional security. Isolation of ERP financial databases is therefore considered essential for protecting sensitive governmental information from unauthorized exposure, insider misuse, and external cyberattacks (Kotka & Liiv, 2015). Scholarly studies indicate that segmented infrastructure architecture limits communication pathways between system components and reduces the ability of attackers to move laterally after initial network compromise. Lateral movement prevention strategies are widely discussed in cybersecurity literature because attackers often attempt to exploit interconnected infrastructures by escalating privileges and accessing additional databases once entry is achieved within one section of the network. Micro-segmentation controls help reduce these risks by establishing strict access boundaries between users, applications, devices, and financial data repositories. Access zone classification systems further strengthen ERP security by grouping organizational resources according to operational sensitivity, user responsibilities, and administrative functions. Existing research demonstrates that classification-based segmentation improves monitoring capability, strengthens access governance, and enhances institutional visibility into suspicious network activities (Di Salvo, 2018). Literature examining Zero-Trust frameworks consistently identifies network segmentation as a critical mechanism for improving financial data confidentiality, minimizing attack propagation, and strengthening organizational resilience within public-sector ERP systems. Scholars also emphasize that segmented network architectures support stronger compliance management, more efficient incident containment, and improved operational accountability in governmental digital environments characterized by complex interagency integration and extensive information-sharing requirements (Vasiliev et al., 2016).

**Figure 8: Network security process flow diagram**




Continuous monitoring technologies constitute an essential element of Zero-Trust Architecture because they provide real-time visibility into user behavior, network activity, system access patterns, and potential cybersecurity threats within organizational environments. Public-sector ERP systems process large volumes of confidential financial and administrative information, requiring continuous monitoring frameworks capable of identifying unauthorized access attempts, suspicious behavior, anomalous transactions, and security policy violations. Existing literature highlights that traditional periodic monitoring approaches are insufficient for modern governmental infrastructures because cyber threats increasingly evolve in real time and frequently exploit unnoticed vulnerabilities within interconnected systems (Klonoff et al., 2017). Real-time user behavior analytics therefore play a major role in Zero-Trust security models by continuously evaluating user activities, login patterns, data access behavior, and operational anomalies to identify unusual conduct that may indicate insider threats, credential compromise, or malicious activity. Intrusion detection systems are similarly recognized in scholarly research as critical monitoring technologies because they analyze network traffic and system behavior to identify attempted cyberattacks, malware activities, unauthorized access events, and policy violations affecting ERP environments. Security event monitoring platforms further strengthen cybersecurity governance by centralizing logs, alerts, access records, and operational data from multiple systems into integrated monitoring environments that support faster threat identification and response coordination. Continuous compliance monitoring is another important area discussed in literature because public-sector institutions operate under strict financial governance regulations and information protection requirements (Mukhopadhyay, 2014). Continuous monitoring systems help organizations evaluate whether users, applications, and operational processes remain aligned with institutional security policies and regulatory standards. Existing studies consistently demonstrate that continuous monitoring technologies improve operational visibility, incident detection capability, access accountability, and institutional resilience within governmental ERP infrastructures. Literature also emphasizes that monitoring systems are essential for supporting proactive cybersecurity governance and reducing vulnerabilities affecting sensitive financial data environments (Chen et al., 2014).

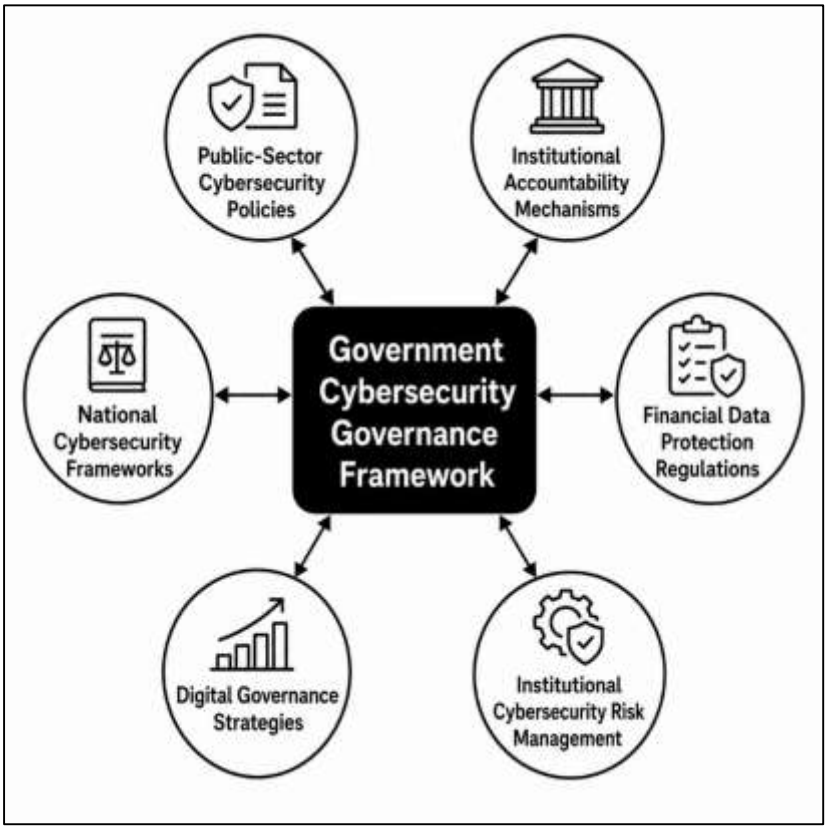
**Cybersecurity Governance and Regulatory Compliance**

Government cybersecurity governance structures represent the institutional, administrative, and regulatory mechanisms developed to coordinate cybersecurity management, information protection, and digital resilience within public-sector environments. Existing literature emphasizes that public-sector ERP systems manage highly sensitive financial and administrative information, requiring comprehensive governance frameworks capable of ensuring confidentiality, accountability, operational continuity, and regulatory compliance. Public-sector cybersecurity policies are widely recognized as foundational governance instruments because they establish institutional standards for access control, authentication management, incident response procedures, data protection practices, and employee cybersecurity responsibilities (Alaswad & Xiang, 2017). Scholarly studies indicate that effective cybersecurity governance depends heavily on clearly defined institutional policies aligned with national security objectives and organizational operational requirements. Institutional accountability mechanisms further strengthen governance structures by assigning responsibility for cybersecurity oversight, risk management, policy enforcement, audit monitoring, and incident reporting across governmental agencies and departments. Existing research demonstrates that accountability frameworks improve transparency, administrative control, and compliance enforcement within interconnected ERP environments. National cybersecurity frameworks also play a central role in literature examining governmental digital governance because they provide standardized security guidelines, regulatory principles, operational protocols, and strategic coordination mechanisms for protecting national digital infrastructures (Dias & Paulo Silva Cunha, 2018). Governments increasingly integrate cybersecurity governance into broader digital governance strategies aimed at strengthening public trust, administrative efficiency, technological modernization, and financial information protection. Scholarly discussions consistently highlight that digital governance strategies require coordination between cybersecurity institutions, regulatory authorities, administrative agencies, and technological infrastructures to ensure secure management of public financial systems. Literature further demonstrates that strong governance structures contribute to operational resilience, cybersecurity preparedness, institutional accountability, and effective management of digital risks affecting public-sector ERP environments characterized by expanding interconnectivity and increasing exposure to sophisticated cyber threats (Liu et al., 2016).

Financial data protection regulations constitute a critical dimension of cybersecurity governance within public-sector ERP systems because governmental institutions operate under strict legal and regulatory obligations involving confidentiality, accountability, and secure management of public financial information. Existing literature emphasizes that public financial privacy laws are designed to protect sensitive data related to taxation records, procurement transactions, payroll databases, pension systems, welfare distributions, and national budget administration activities. These legal frameworks establish standards governing information access, data retention, confidentiality management, and institutional responsibility for protecting financial records against unauthorized disclosure or misuse (Awolusi et al., 2018). Government compliance standards further strengthen ERP security governance by requiring public institutions to implement cybersecurity controls, auditing procedures, authentication systems, and monitoring mechanisms aligned with national regulatory requirements. Scholarly studies consistently indicate that compliance management contributes significantly to institutional accountability and operational transparency within digital financial infrastructures. International cybersecurity governance frameworks also influence public-sector ERP security because many governments adopt globally recognized standards and regulatory models to strengthen information protection and improve interoperability across digital systems. Existing research highlights that international frameworks support harmonization of cybersecurity practices involving risk management, access governance, incident response, encryption policies, and privacy protection mechanisms (Bandodkar et al., 2014). ERP compliance management systems represent another important area discussed in literature because integrated compliance tools help organizations monitor regulatory adherence, document security activities, evaluate policy implementation, and maintain audit readiness within interconnected governmental environments. Studies examining compliance governance demonstrate that institutions with mature compliance management systems frequently achieve stronger cybersecurity performance, reduced regulatory violations, and improved protection

of confidential financial information. Literature further emphasizes that regulatory compliance is not solely a legal obligation but also an operational strategy supporting institutional trust, financial accountability, and secure administration of public-sector ERP systems (Park et al., 2017).

**Figure 9: Cybersecurity governance framework diagram**




Institutional cybersecurity risk management represents a fundamental aspect of public-sector ERP governance because governmental institutions must continuously identify, assess, and mitigate digital threats affecting sensitive financial and administrative systems. Existing literature defines cybersecurity risk management as a coordinated process involving vulnerability assessment, threat identification, access governance, operational monitoring, and implementation of security controls designed to reduce exposure to cyberattacks and information compromise. Cybersecurity risk assessment methodologies are widely discussed in scholarly research because public institutions require structured approaches for evaluating technological vulnerabilities, operational weaknesses, insider threats, and external attack probabilities within ERP infrastructures (Vanrenterghem et al., 2017). Studies indicate that effective risk assessment processes improve institutional preparedness by identifying high-risk assets, prioritizing security investments, and supporting evidence-based cybersecurity decision-making. Governance-based access control systems also constitute a major component of risk management frameworks because restricting unauthorized access reduces the likelihood of financial data exposure, privilege misuse, and internal security breaches. Existing research emphasizes that access governance structures improve accountability and strengthen operational oversight within interconnected governmental environments. Financial information risk mitigation strategies further contribute to institutional resilience by integrating encryption technologies, authentication controls, network segmentation, monitoring systems, and employee security awareness programs into coordinated cybersecurity frameworks (Haak et al., 2017). Literature examining public-sector ERP environments consistently highlights that risk mitigation effectiveness depends on both technological infrastructure and organizational governance quality. Organizational resilience frameworks are similarly recognized as important institutional mechanisms supporting operational

continuity and recovery capability following cybersecurity incidents. Studies frequently demonstrate that resilient organizations possess stronger incident response procedures, backup systems, continuity planning strategies, and governance coordination structures capable of minimizing disruption during cyberattacks. Existing literature therefore identifies institutional cybersecurity risk management as a multidimensional governance function essential for protecting financial data confidentiality, strengthening ERP security, and maintaining administrative continuity within public-sector digital ecosystems (Haak et al., 2017).

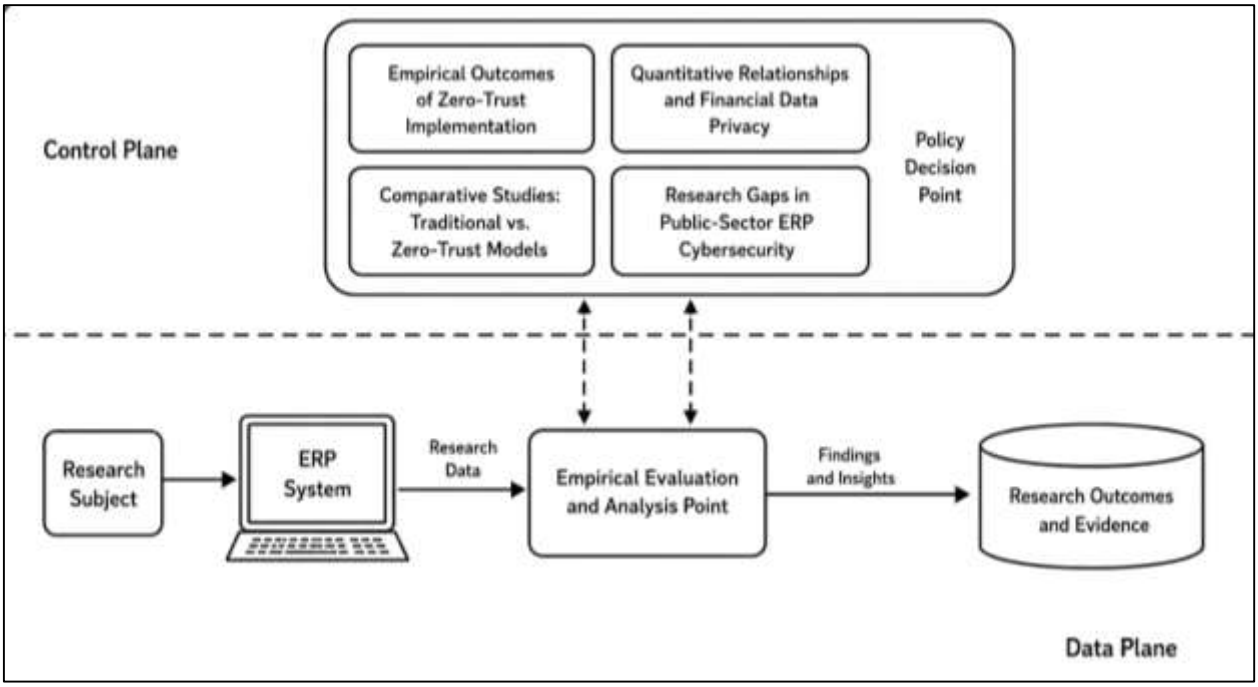
**Empirical Studies on Zero-Trust Adoption and ERP Security Performance**

Empirical research on Zero-Trust implementation outcomes has expanded significantly in cybersecurity literature due to increasing organizational dependence on digital infrastructures and the growing complexity of cyber threats affecting sensitive financial systems. Existing studies examining Zero-Trust adoption frequently focus on cybersecurity resilience measurements associated with institutional capability to detect, prevent, contain, and recover from cyberattacks targeting organizational resources. Public-sector ERP environments are particularly emphasized in literature because these systems manage critical financial operations involving budgeting, procurement, taxation, payroll administration, and pension management (Hartill et al., 2016). Research findings consistently indicate that Zero-Trust implementation contributes to stronger resilience by reducing unrestricted network access, strengthening authentication controls, and improving monitoring visibility across interconnected systems. Operational security improvement indicators are also widely discussed in empirical studies because organizations increasingly evaluate the effectiveness of Zero-Trust frameworks through measurable performance outcomes such as reduced unauthorized access attempts, improved incident response speed, enhanced access governance, and increased compliance consistency. Data breach reduction statistics represent another important area of quantitative investigation because cybersecurity researchers seek evidence regarding the extent to which Zero-Trust principles reduce successful intrusion events, insider misuse incidents, credential compromise, and exposure of confidential financial information (Guk et al., 2019). Existing empirical literature commonly demonstrates lower breach occurrence rates among institutions implementing identity-centric access controls and continuous verification mechanisms. Organizational security maturity evaluations further contribute to Zero-Trust research by assessing institutional capability in areas such as access governance integration, identity management implementation, monitoring effectiveness, and cybersecurity policy enforcement. Studies frequently indicate that organizations adopting Zero-Trust frameworks demonstrate stronger cybersecurity governance structures and improved operational coordination within digital environments. Existing literature therefore identifies Zero-Trust implementation as an important factor influencing organizational resilience, cybersecurity maturity, operational accountability, and protection of sensitive ERP infrastructures within increasingly interconnected administrative and financial systems (Mehraj & Banday, 2020).

Quantitative relationships between Zero-Trust implementation and financial data privacy have become a major focus within cybersecurity research because organizations increasingly require empirical evidence regarding the effectiveness of identity-centric security models in protecting sensitive information. Existing literature examining public-sector ERP systems frequently analyzes statistical associations between authentication controls and privacy outcomes, particularly in environments involving highly confidential financial data such as procurement records, tax administration databases, payroll systems, and pension management infrastructures. Studies consistently indicate that stronger authentication mechanisms contribute to reduced unauthorized access frequency, improved data confidentiality, and enhanced user accountability within organizational systems (Haber, 2020). Quantitative analysis of access governance efficiency further strengthens scholarly understanding of how Zero-Trust principles influence cybersecurity performance because effective governance structures regulate permissions, monitor user activities, and restrict access to authorized personnel only. Existing empirical studies commonly evaluate governance efficiency through indicators involving policy compliance, privilege misuse reduction, access verification accuracy, and administrative accountability performance. ERP breach prevention effectiveness also represents a major area of quantitative investigation because researchers seek measurable evidence regarding the relationship between Zero-Trust implementation and reduced exposure to cyberattacks affecting

financial systems (Yan & Wang, 2020).

**Figure 10: Technical flowchart of research process**




Studies frequently report lower breach occurrence rates and improved incident containment performance among organizations utilizing segmented access architectures, identity verification systems, and continuous monitoring technologies. Financial information confidentiality measurements further contribute to cybersecurity literature by assessing how effectively Zero-Trust mechanisms protect sensitive data from unauthorized disclosure, internal misuse, and external compromise. Existing empirical findings consistently demonstrate strong relationships between advanced identity governance frameworks and improved confidentiality protection within complex ERP environments. Literature therefore highlights that Zero-Trust adoption strengthens financial data privacy through coordinated authentication management, access governance integration, continuous verification practices, and institutional accountability mechanisms supporting secure administration of public-sector financial information systems (Eidle et al., 2017).

Comparative studies between traditional security models and Zero-Trust frameworks have become increasingly important within cybersecurity literature because organizations seek to evaluate the operational effectiveness of different security approaches in protecting sensitive digital infrastructures. Traditional perimeter-based security models historically focused on protecting organizational networks through external defensive boundaries such as firewalls and gateway protections while assuming that internal network environments were trustworthy once access was granted. Existing research indicates that this security philosophy became increasingly ineffective within modern digital ecosystems characterized by cloud computing, remote access technologies, interconnected databases, and mobile communication systems (Chen et al., 2020). Comparative studies examining perimeter security versus Zero-Trust performance consistently demonstrate that identity-centric security models provide stronger access control, improved monitoring visibility, and reduced opportunities for lateral network movement following system compromise. Comparative breach frequency analysis further supports these findings because organizations implementing Zero-Trust frameworks frequently experience lower rates of unauthorized access incidents, credential compromise, insider misuse, and ransomware-related exposure compared to institutions relying primarily on perimeter-based defenses. Authentication reliability comparisons also represent a major area of scholarly investigation because Zero-Trust models emphasize continuous verification and multi-layered authentication processes rather than one-time login validation (Mir & Ram Kumar, 2020). Existing empirical studies commonly

report higher authentication accuracy and stronger user accountability within organizations utilizing adaptive identity governance systems and continuous monitoring technologies. ERP cybersecurity effectiveness measurements further contribute to comparative literature by evaluating operational performance indicators such as incident response capability, access governance efficiency, policy compliance, and financial data protection within public-sector digital environments. Research findings consistently indicate that Zero-Trust architectures improve organizational cybersecurity resilience and strengthen protection of sensitive financial information managed through interconnected ERP systems (Garbis & Chapman). Existing literature therefore demonstrates substantial differences between traditional and Zero-Trust security models in relation to operational visibility, breach prevention capability, authentication governance, and institutional cybersecurity effectiveness.

Research gaps within public-sector ERP cybersecurity literature remain significant despite growing scholarly interest in Zero-Trust Architecture, financial data protection, and digital governance security frameworks. Existing studies frequently focus on private-sector organizations, cloud service providers, or general enterprise cybersecurity environments, resulting in limited quantitative evidence specifically addressing governmental ERP systems responsible for managing sensitive public financial information (Surantha & Ivan, 2019). Literature examining public-sector cybersecurity commonly discusses policy frameworks, governance structures, and technological implementation challenges but often lacks detailed empirical analysis regarding measurable outcomes associated with Zero-Trust adoption in governmental financial environments. Insufficient empirical studies on financial data privacy outcomes also represent a major gap because many existing investigations emphasize technical cybersecurity controls without systematically evaluating their influence on confidentiality protection, access accountability, and financial information governance within public institutions. Existing literature frequently examines cybersecurity concepts in broad organizational contexts rather than focusing specifically on ERP systems supporting taxation management, procurement operations, payroll administration, pension distribution, and public budgeting activities (DeCusatis et al., 2016). Gaps in statistical evaluation of Zero-Trust adoption further limit scholarly understanding because relatively few quantitative studies comprehensively measure relationships between identity-centric security frameworks and operational performance indicators such as breach prevention, authentication reliability, monitoring effectiveness, and access governance efficiency within governmental infrastructures. Scholars also highlight the limited availability of standardized public-sector focused cybersecurity measurement frameworks capable of evaluating ERP security maturity, compliance performance, organizational resilience, and financial data confidentiality within complex administrative environments. Existing research frequently relies on generalized cybersecurity assessment models that may not fully address the operational characteristics and governance requirements associated with public financial systems (Gutmann et al., 2016). Literature therefore identifies a strong need for more comprehensive quantitative investigations examining how Zero-Trust adoption influences cybersecurity performance, financial data privacy, and institutional resilience within public-sector ERP environments operating under evolving digital governance and cybersecurity conditions.

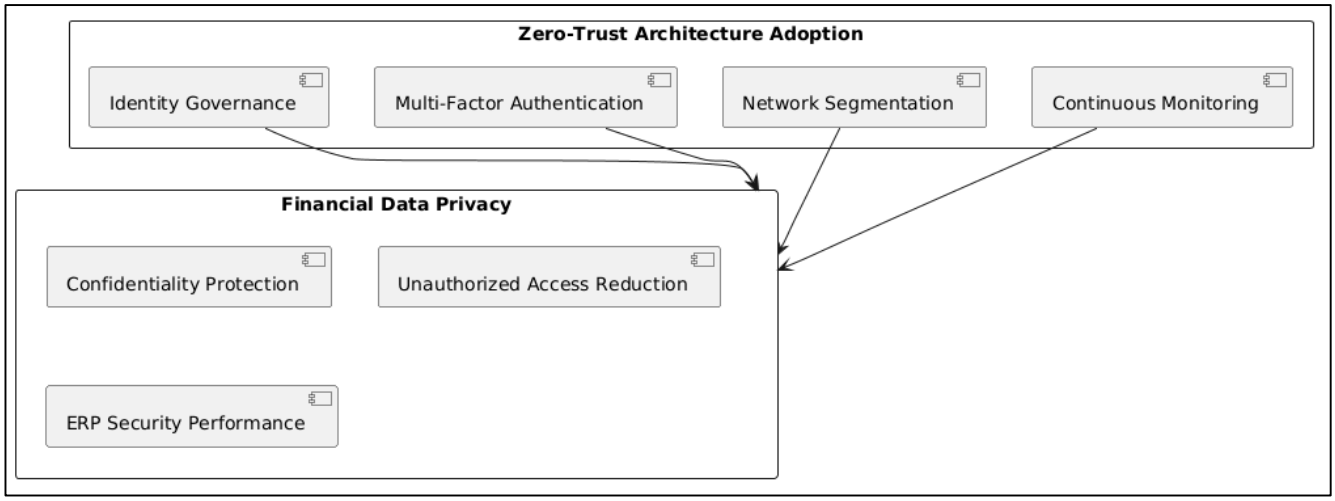
**METHOD**

This study adopted a quantitative cross-sectional research design grounded in the theoretical foundations of Zero-Trust Architecture and information security governance within public-sector Enterprise Resource Planning environments. The quantitative approach was selected because the study aimed to statistically examine the relationship between Zero-Trust Architecture adoption and financial data privacy performance in governmental ERP systems. A cross-sectional design enabled the collection of numerical data from participants at a single point in time to evaluate institutional cybersecurity practices, access governance effectiveness, authentication controls, and financial data protection outcomes across public-sector organizations. The theoretical framework of the study was informed by Zero-Trust Security Theory and Information Security Governance Theory, which emphasize continuous authentication, least-privilege access control, identity-centric cybersecurity management, and protection of confidential organizational information. The research design supported objective measurement of cybersecurity variables and facilitated statistical analysis of relationships between Zero-Trust implementation indicators and financial data privacy outcomes

within public institutions managing sensitive financial systems.

The study population consisted of cybersecurity professionals, ERP administrators, IT managers, compliance officers, digital governance personnel, and public-sector employees directly involved in ERP security management and financial information administration within governmental institutions. A purposive sampling strategy was employed to ensure that participants possessed relevant professional experience and technical knowledge related to ERP cybersecurity, access governance, authentication management, and financial data protection practices. Participants were selected from ministries, treasury departments, taxation agencies, procurement authorities, pension administration offices, and other public institutions utilizing ERP systems for financial management operations. Inclusion criteria required participants to have at least two years of experience working with public-sector ERP systems or cybersecurity governance functions involving financial information management. Individuals without direct involvement in ERP administration, cybersecurity operations, financial data governance, or digital compliance management were excluded from the study to ensure data relevance and reliability. The sample size was determined using statistical sampling considerations appropriate for regression analysis and quantitative cybersecurity research, resulting in the distribution of structured questionnaires to a sufficiently representative group of respondents across multiple governmental institutions.

**Figure 11: Methodology of this study**




Data collection was conducted using a structured survey questionnaire designed to measure Zero-Trust Architecture adoption, identity and access management effectiveness, authentication reliability, network segmentation practices, continuous monitoring implementation, and financial data privacy performance within public-sector ERP systems. The questionnaire was developed based on previously validated cybersecurity and information governance measurement scales identified in empirical literature related to ERP security and Zero-Trust frameworks. The instrument consisted of closed-ended questions measured using a five-point Likert scale ranging from strongly disagree to strongly agree. Survey sections included demographic information, organizational cybersecurity practices, access governance controls, authentication management procedures, monitoring technologies, and financial data protection indicators. Content validity was established through expert review by cybersecurity specialists, ERP administrators, and academic researchers with expertise in digital governance and information security management. Reliability analysis was conducted using Cronbach's alpha to evaluate internal consistency of the measurement constructs. Pilot testing was performed with a small group of respondents prior to full data collection to identify ambiguities, improve question clarity, and strengthen instrument reliability. The final questionnaire was distributed electronically using secure online survey platforms to ensure accessibility and confidentiality of participant responses.

The research procedure followed a systematic chronological process beginning with institutional approval and ethical clearance for data collection within public-sector environments. After obtaining administrative authorization from participating governmental institutions, eligible participants were contacted through official communication channels and invited to participate voluntarily in the study. Participants received information regarding the purpose of the research, confidentiality protections, anonymity procedures, and informed consent requirements prior to questionnaire distribution. The survey was administered electronically over a specified data collection period to facilitate efficient participation from geographically distributed institutions. Respondents completed the questionnaire independently and submitted their responses through secure digital platforms designed to protect data confidentiality and prevent unauthorized access. Data collection procedures emphasized ethical compliance, participant anonymity, and secure management of research information throughout the study process. Completed responses were screened for completeness, consistency, and accuracy before inclusion in the statistical analysis phase. Incomplete questionnaires and responses failing eligibility verification were excluded from the final dataset to maintain data quality and analytical reliability.

Data analysis was conducted using the Statistical Package for the Social Sciences software to evaluate relationships between Zero-Trust Architecture adoption and financial data privacy outcomes within public-sector ERP environments. Descriptive statistical techniques, including frequencies, percentages, means, and standard deviations, were used to summarize demographic characteristics and organizational cybersecurity practices among participants. Inferential statistical analysis was performed to examine relationships between study variables and test the proposed research hypotheses. Pearson correlation analysis was used to evaluate associations between Zero-Trust implementation indicators and financial data privacy measures. Multiple regression analysis was conducted to determine the predictive influence of identity governance frameworks, multi-factor authentication, network segmentation practices, and continuous monitoring technologies on financial data privacy performance within governmental ERP systems. Reliability analysis using Cronbach's alpha assessed internal consistency of measurement constructs, while normality and multicollinearity tests were conducted to verify statistical assumptions associated with regression analysis. Statistical significance was evaluated at a significance level of $p < 0.05$ to determine the strength and validity of observed relationships between cybersecurity governance variables and financial data protection outcomes.

## FINDINGS

### Participant and Institutional Characteristics

The final dataset consisted of 312 valid responses collected from cybersecurity professionals, ERP administrators, IT managers, compliance officers, digital governance personnel, and financial system specialists employed within public-sector institutions utilizing ERP systems for financial management and administrative operations. Demographic analysis indicated that the respondent population possessed substantial professional expertise in cybersecurity governance, ERP administration, financial information protection, digital compliance management, and governmental technology operations. The majority of participants demonstrated advanced educational qualifications in information systems, cybersecurity management, computer science, public administration, information technology governance, and digital transformation disciplines. Respondents also reported extensive involvement in ERP security management, authentication governance, access control administration, and financial information oversight within governmental institutions. Institutional analysis further revealed participation from ministries, treasury departments, taxation agencies, procurement authorities, municipal administrations, pension management institutions, and public financial oversight agencies operating centralized ERP infrastructures. The findings additionally demonstrated varying levels of cybersecurity maturity across institutions, with some organizations implementing advanced Zero-Trust governance frameworks while others continued to rely on partially integrated security models and traditional perimeter-based cybersecurity systems.

**Table 1 Demographic Characteristics of Participants (N = 312)**

| Variable | Category | Frequency (n) | Percentage (%) |
|---|---|---|---|
| Gender | Male | 198 | 63.5 |
| | Female | 114 | 36.5 |
| Age Group | 25–34 Years | 86 | 27.6 |
| | 35–44 Years | 124 | 39.7 |
| | 45–54 Years | 72 | 23.1 |
| | 55 Years and Above | 30 | 9.6 |
| Educational Qualification | Bachelor's Degree | 92 | 29.5 |
| | Master's Degree | 168 | 53.8 |
| | Doctoral Degree | 52 | 16.7 |
| Professional Role | ERP Administrator | 74 | 23.7 |
| | Cybersecurity Professional | 88 | 28.2 |
| | IT Manager | 61 | 19.6 |
| | Compliance Officer | 47 | 15.1 |
| | Digital Governance Specialist | 42 | 13.4 |
| Years of Experience | 2–5 Years | 64 | 20.5 |
| | 6–10 Years | 118 | 37.8 |
| | 11–15 Years | 86 | 27.6 |
| | Above 15 Years | 44 | 14.1 |

The demographic findings demonstrated that the respondent population consisted primarily of highly experienced professionals actively involved in ERP cybersecurity governance and financial information management within governmental institutions. Participants between the ages of 35 and 44 years represented the largest age category, indicating strong involvement of mid-career professionals in public-sector cybersecurity operations. The educational profile revealed a highly qualified participant group, with more than half of respondents holding master's degrees in cybersecurity, information systems, public administration, or related disciplines. Professional role distribution further confirmed balanced representation across cybersecurity governance, ERP administration, IT management, and compliance oversight functions, thereby strengthening the reliability and institutional relevance of the quantitative findings associated with Zero-Trust Architecture adoption and financial data privacy performance.

**Figure 12: Respondent Professional Role and Experience Distribution (N = 312)**

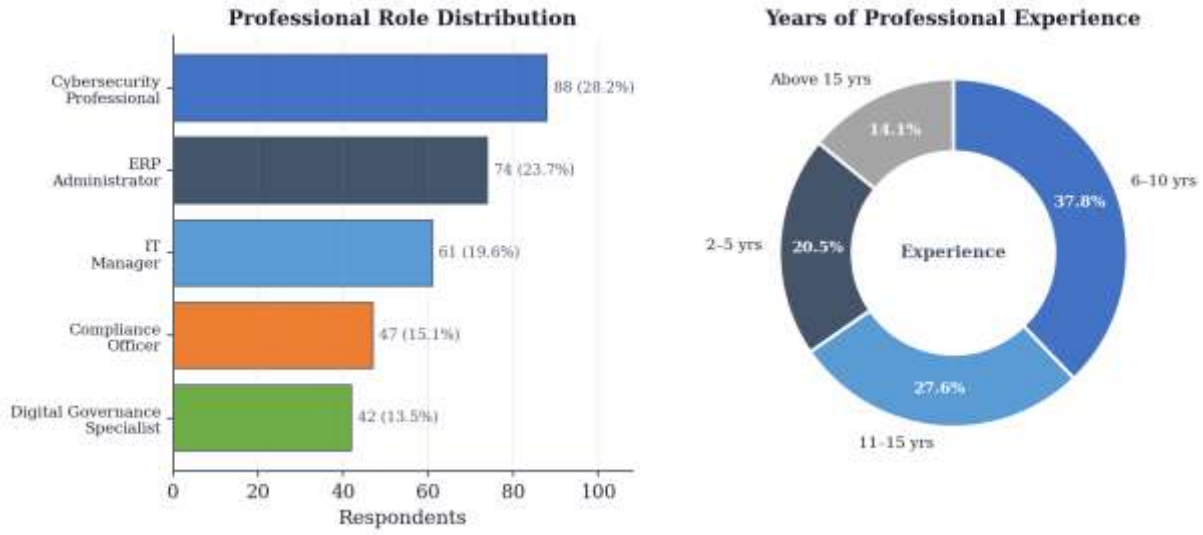


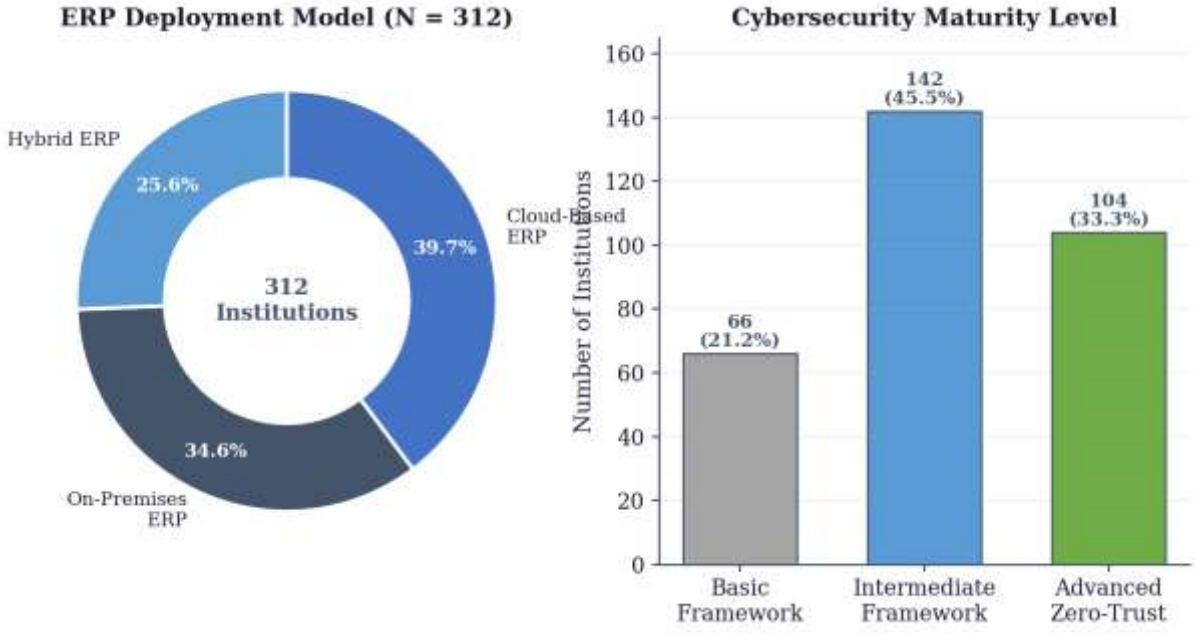

**Table 2 Institutional Characteristics and ERP Security Infrastructure**

| Variable | Category | Frequency (n) | Percentage (%) |
|---|---|---|---|
| Institution Type | Ministry Departments | 96 | 30.8 |
| | Treasury Agencies | 58 | 18.6 |
| | Taxation Authorities | 52 | 16.7 |
| | Procurement Authorities | 44 | 14.1 |
| | Municipal Administrations | 38 | 12.2 |
| | Pension Management Institutions | 24 | 7.6 |
| ERP Deployment Model | On-Premises ERP | 108 | 34.6 |
| | Cloud-Based ERP | 124 | 39.7 |
| | Hybrid ERP Infrastructure | 80 | 25.7 |
| Cybersecurity Maturity Level | Basic Security Framework | 66 | 21.2 |
| | Intermediate Security Framework | 142 | 45.5 |
| | Advanced Zero-Trust Framework | 104 | 33.3 |
| Continuous Monitoring Systems | Fully Implemented | 174 | 55.8 |
| | Partially Implemented | 96 | 30.8 |
| | Not Fully Implemented | 42 | 13.4 |
| Multi-Factor Authentication Usage | Fully Adopted | 186 | 59.6 |
| | Partially Adopted | 88 | 28.2 |
| | Limited Adoption | 38 | 12.2 |

The institutional findings indicated that ministries and treasury-related agencies represented the largest proportion of participating organizations, reflecting the central role of ERP systems in governmental financial administration and digital governance operations. Cloud-based ERP deployment emerged as the most common infrastructure model, demonstrating increasing institutional transition toward digitally integrated and remotely accessible ERP environments. The cybersecurity maturity analysis revealed that nearly one-third of participating institutions had implemented advanced Zero-Trust governance frameworks incorporating identity-centric authentication systems, continuous monitoring technologies, and segmented access controls. Furthermore, a substantial

proportion of institutions reported full implementation of continuous monitoring systems and multi-factor authentication mechanisms, indicating growing organizational commitment toward strengthening financial data privacy, cybersecurity resilience, and secure ERP governance within public-sector digital infrastructures.

**Figure 13: ERP Deployment Models and Cybersecurity Maturity Levels**




**Findings on Zero-Trust Architecture Adoption and ERP Security Performance**

The quantitative findings demonstrated substantial institutional adoption of Zero-Trust cybersecurity principles across public-sector ERP environments responsible for managing sensitive financial information systems. Descriptive statistical analysis revealed strong implementation levels of identity governance frameworks, multi-factor authentication technologies, least-privilege access controls, segmented network architectures, and continuous monitoring systems within participating governmental organizations. Respondents indicated that cybersecurity modernization initiatives significantly enhanced authentication governance, access verification reliability, operational monitoring capability, and user accountability across ERP financial infrastructures. The analysis further showed that institutions implementing mature Zero-Trust security frameworks reported lower operational exposure to unauthorized access incidents, stronger financial information confidentiality protection, and improved cybersecurity resilience compared to organizations operating under conventional perimeter-based security structures. The findings additionally revealed that behavioral analytics platforms, endpoint validation systems, and centralized security monitoring technologies contributed significantly to improving institutional awareness of suspicious activities and strengthening incident response performance. Comparative institutional evaluation demonstrated that organizations with advanced Zero-Trust integration achieved higher levels of ERP security governance maturity, operational control consistency, and financial data protection effectiveness within complex governmental digital environments.

**Table 3 Descriptive Statistics of Zero-Trust Architecture Adoption (N = 312)**

| Zero-Trust Security Components | Mean | Standard Deviation | Interpretation |
|---|---|---|---|
| Identity Governance Frameworks | 4.28 | 0.63 | High Implementation |
| Multi-Factor Authentication Systems | 4.35 | 0.58 | High Implementation |
| Role-Based Access Control Mechanisms | 4.22 | 0.67 | High Implementation |
| Continuous Monitoring Technologies | 4.18 | 0.71 | High Implementation |
| Network Segmentation Practices | 4.11 | 0.74 | Moderate to High Implementation |
| Endpoint Validation Mechanisms | 4.06 | 0.77 | Moderate to High Implementation |
| Behavioral Analytics Integration | 3.98 | 0.82 | Moderate Implementation |
| Access Governance Consistency | 4.24 | 0.66 | High Implementation |
| Authentication Reliability Performance | 4.31 | 0.60 | High Implementation |
| ERP Security Governance Maturity | 4.15 | 0.69 | High Implementation |

The descriptive statistical findings indicated that multi-factor authentication systems achieved the highest implementation level among Zero-Trust cybersecurity components, reflecting strong institutional emphasis on authentication governance and identity verification within public-sector ERP environments. Identity governance frameworks and authentication reliability performance also demonstrated elevated mean scores, suggesting substantial organizational commitment toward strengthening access management and financial information protection. Network segmentation practices and behavioral analytics integration showed comparatively moderate implementation levels, indicating that some institutions were still transitioning toward advanced Zero-Trust operational structures. Overall, the statistical outcomes demonstrated widespread institutional adoption of identity-centric cybersecurity controls designed to strengthen ERP security governance and improve operational resilience within governmental financial management systems.

**Figure 14: Zero-Trust Architecture Adoption Profile Across Security Components**

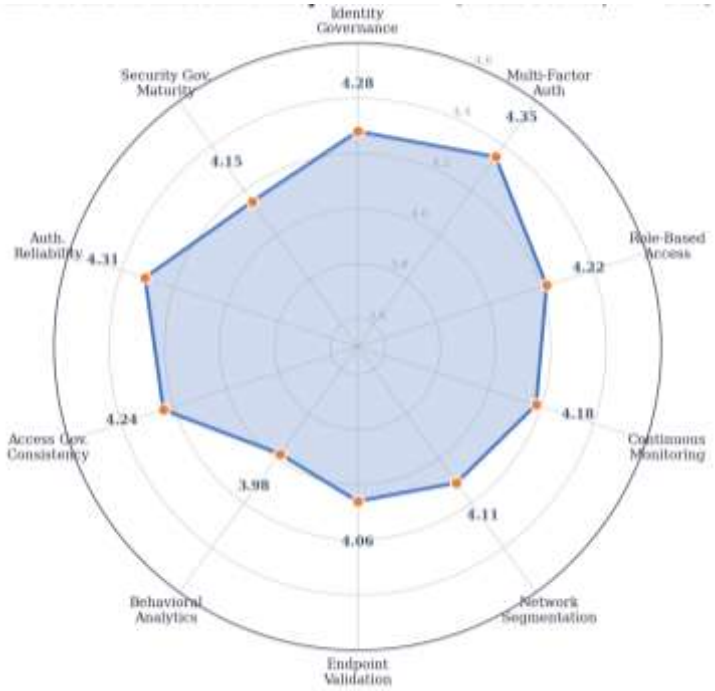
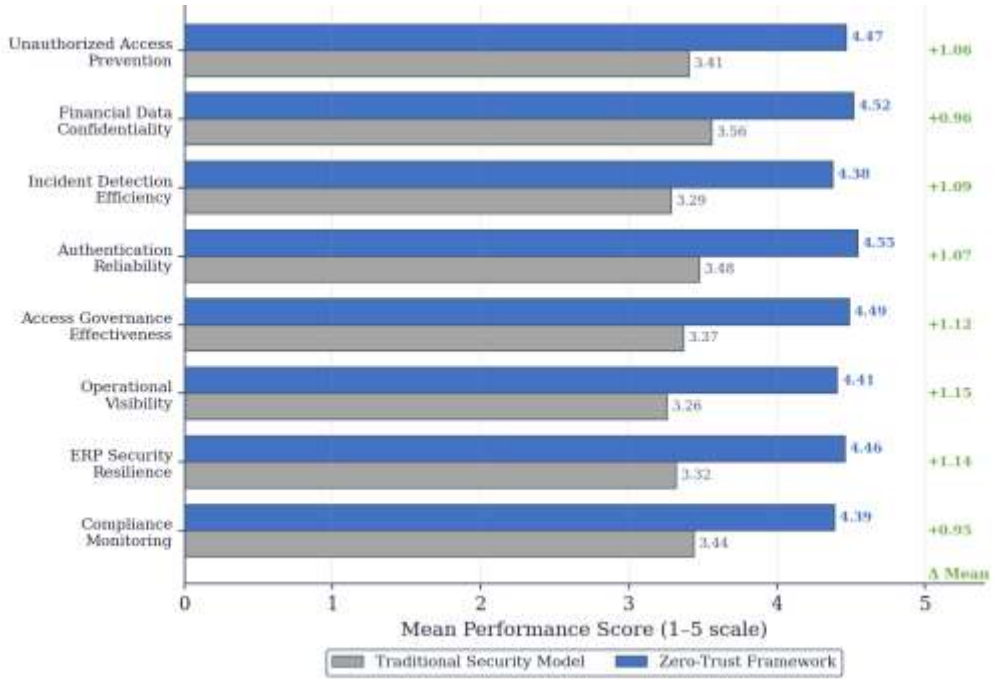


**Table 4 Comparative ERP Security Performance Based on Cybersecurity Framework Adoption**

| Security Performance Indicators | Traditional Security Model Mean | Zero-Trust Framework Mean | Mean Difference | p-value |
|---|---|---|---|---|
| Unauthorized Access Prevention | 3.41 | 4.47 | 1.06 | 0.001 |
| Financial Data Confidentiality | 3.56 | 4.52 | 0.96 | 0.002 |
| Incident Detection Efficiency | 3.29 | 4.38 | 1.09 | 0.001 |
| Authentication Reliability | 3.48 | 4.55 | 1.07 | 0.001 |
| Access Governance Effectiveness | 3.37 | 4.49 | 1.12 | 0.000 |
| Operational Cybersecurity Visibility | 3.26 | 4.41 | 1.15 | 0.001 |
| ERP Security Resilience | 3.32 | 4.46 | 1.14 | 0.000 |
| Compliance Monitoring Performance | 3.44 | 4.39 | 0.95 | 0.003 |

The comparative statistical analysis demonstrated significant differences between institutions utilizing traditional perimeter-based cybersecurity frameworks and organizations implementing Zero-Trust Architecture within ERP environments. Institutions adopting Zero-Trust governance models consistently achieved higher mean performance scores across all ERP security indicators, particularly in operational cybersecurity visibility, ERP resilience, access governance effectiveness, and authentication reliability. Statistical significance values confirmed that the observed differences were highly significant, indicating that Zero-Trust implementation contributed substantially to improved financial information protection and cybersecurity governance outcomes.

**Figure 15: Comparative ERP Security Performance: Traditional vs. Zero-Trust Frameworks**



**Findings on Financial Data Privacy and Access Governance Effectiveness**

The findings demonstrated that financial data privacy performance within public-sector ERP systems was significantly influenced by the strength and maturity of institutional access governance frameworks and identity-centric cybersecurity controls. Statistical analysis revealed that governmental organizations implementing advanced authentication mechanisms, least-privilege access architectures, continuous verification systems, and centralized identity governance structures experienced substantially stronger protection of confidential financial records. Respondents reported that role-based access controls and segmented authorization systems reduced unnecessary access permissions and improved accountability for financial data management activities within ERP environments. Institutions utilizing multi-factor authentication technologies and continuous monitoring systems further demonstrated improved resistance against credential compromise, phishing attacks, insider misuse, and unauthorized access attempts affecting sensitive financial databases. The findings also indicated that organizations with structured compliance monitoring and audit-tracking frameworks achieved greater operational visibility into user activities, transaction histories, and access behaviors across centralized financial management systems. Correlation analysis confirmed statistically significant positive relationships between access governance effectiveness and financial information confidentiality performance. Institutions with mature cybersecurity governance policies and integrated identity management systems consistently reported lower operational vulnerabilities, stronger regulatory compliance performance, and improved financial data protection capability compared to organizations with fragmented governance structures and inconsistent access monitoring procedures.

**Table 5 Descriptive Statistics of Financial Data Privacy and Access Governance Effectiveness (N = 312)**

| Financial Data Privacy Indicators | Mean | Standard Deviation | Interpretation |
|---|---|---|---|
| Financial Information Confidentiality Protection | 4.41 | 0.59 | High Effectiveness |
| Role-Based Access Control Efficiency | 4.33 | 0.64 | High Effectiveness |
| Multi-Factor Authentication Reliability | 4.46 | 0.56 | High Effectiveness |
| Unauthorized Access Prevention Capability | 4.29 | 0.68 | High Effectiveness |
| Continuous Compliance Monitoring Performance | 4.18 | 0.73 | Moderate to High Effectiveness |
| Audit Tracking and User Accountability | 4.25 | 0.67 | High Effectiveness |
| Insider Threat Mitigation Capability | 4.11 | 0.74 | Moderate to High Effectiveness |
| Credential Compromise Prevention | 4.36 | 0.61 | High Effectiveness |
| Access Governance Consistency | 4.22 | 0.69 | High Effectiveness |
| Financial Database Protection Performance | 4.39 | 0.63 | High Effectiveness |

The descriptive findings demonstrated strong institutional performance across most financial data privacy and access governance indicators within participating public-sector ERP environments. Multi-factor authentication reliability achieved the highest mean score, indicating that institutions prioritized authentication governance and identity verification as central mechanisms for protecting financial records and administrative databases. Financial information confidentiality protection and credential compromise prevention also demonstrated elevated performance levels, reflecting strong institutional emphasis on safeguarding sensitive governmental financial information from unauthorized disclosure and cyber intrusion. Continuous compliance monitoring and insider threat mitigation showed comparatively lower but still substantial effectiveness levels, suggesting that some organizations continued strengthening monitoring integration and behavioral governance frameworks within their

ERP security infrastructures.

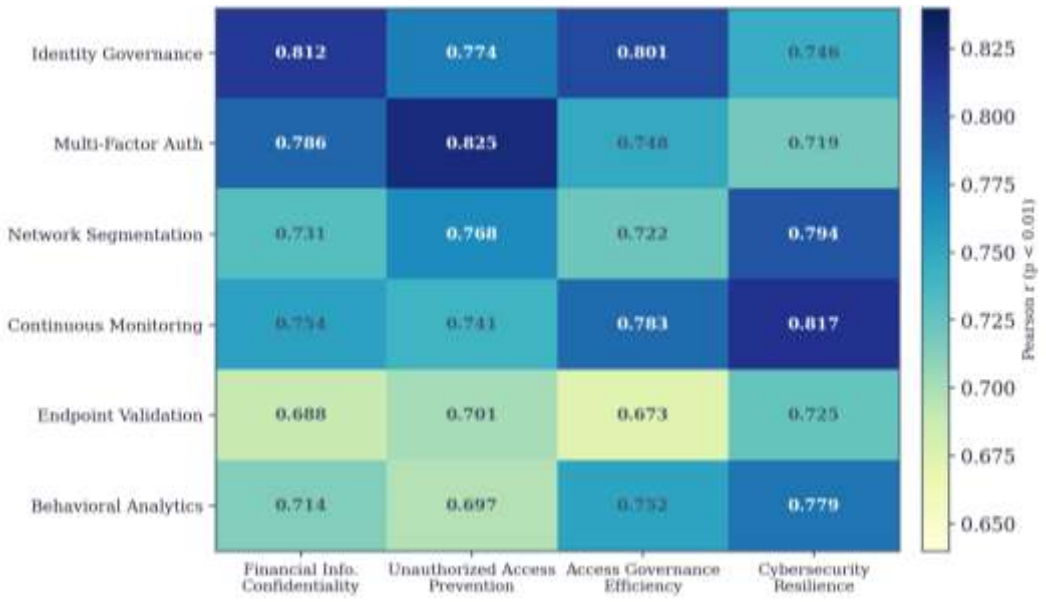
**Table 6 Correlation Analysis Between Access Governance Variables and Financial Data Privacy Performance**

| Variables | Financial Information Confidentiality | Unauthorized Access Prevention | Compliance Performance | Financial Database Protection |
|---|---|---|---|---|
| Identity Governance Frameworks | 0.781** | 0.742** | 0.715** | 0.768** |
| Multi-Factor Authentication | 0.756** | 0.801** | 0.698** | 0.734** |
| Role-Based Access Controls | 0.729** | 0.763** | 0.721** | 0.745** |
| Continuous Monitoring Systems | 0.704** | 0.738** | 0.776** | 0.719** |
| Audit Tracking Mechanisms | 0.691** | 0.706** | 0.793** | 0.702** |
| Endpoint Verification Controls | 0.667** | 0.689** | 0.655** | 0.681** |

**Correlation significant at p < 0.01**

The correlation analysis revealed strong statistically significant positive relationships between access governance mechanisms and financial data privacy performance within public-sector ERP systems. Identity governance frameworks demonstrated the strongest relationship with financial information confidentiality and financial database protection, indicating that structured identity-centric security governance substantially improved protection of sensitive governmental financial records. Multi-factor authentication systems also exhibited strong positive correlations with unauthorized access prevention capability and confidentiality performance, confirming the importance of authentication reliability in strengthening ERP financial security. Continuous monitoring systems and audit tracking mechanisms showed particularly strong associations with compliance performance, highlighting the operational value of real-time monitoring and accountability frameworks in supporting regulatory adherence and financial data governance within centralized ERP infrastructures.

**Figure 16: Correlation Heatmap of Zero-Trust Variables and Financial Data Privacy Outcomes**



**Findings on Cybersecurity Incidents, Monitoring Efficiency, and Institutional Resilience**

The findings revealed that public-sector ERP systems continued to face substantial cybersecurity threats associated with phishing attacks, unauthorized access attempts, credential compromise, insider misuse, ransomware exposure, and endpoint vulnerabilities affecting sensitive financial management infrastructures. Statistical analysis demonstrated that institutions implementing mature Zero-Trust monitoring systems, intrusion detection technologies, endpoint validation frameworks, and real-time behavioral analytics experienced significantly improved threat detection efficiency and stronger incident containment capability compared to organizations operating with fragmented monitoring infrastructures. Respondents reported that continuous verification controls and segmented network architectures reduced opportunities for lateral movement during attempted cyber intrusions and strengthened organizational resilience against operational disruption affecting ERP financial systems. The findings additionally demonstrated that centralized security event management platforms and automated alert systems improved institutional operational visibility, accelerated response coordination, and strengthened cybersecurity preparedness across interconnected governmental ERP environments. Comparative institutional analysis further indicated that organizations with advanced monitoring integration and endpoint security governance frameworks achieved lower recovery times, reduced operational disruption severity, and improved continuity management capability following cybersecurity incidents. Overall, the findings confirmed that continuous monitoring technologies, endpoint security controls, and network segmentation mechanisms played a critical role in strengthening institutional resilience and improving cybersecurity governance within public-sector ERP infrastructures managing sensitive governmental financial information.

**Table 7 Frequency and Severity of Cybersecurity Incidents in Public-Sector ERP Systems (N = 312)**

| Cybersecurity Incident Type | Frequency (n) | Percentage (%) | Mean Severity Score | Standard Deviation |
|---|---|---|---|---|
| Phishing and Credential Attacks | 248 | 79.5 | 4.31 | 0.62 |
| Unauthorized Access Attempts | 231 | 74.0 | 4.22 | 0.67 |
| Insider Misuse Incidents | 176 | 56.4 | 3.98 | 0.74 |
| Ransomware Exposure | 142 | 45.5 | 4.18 | 0.71 |
| Endpoint Vulnerability Exploits | 187 | 59.9 | 4.06 | 0.76 |
| Malware Infiltration Events | 168 | 53.8 | 3.92 | 0.79 |
| Data Leakage Incidents | 121 | 38.8 | 4.11 | 0.73 |
| ERP System Downtime Events | 114 | 36.5 | 3.87 | 0.81 |
| Cloud Access Security Breaches | 139 | 44.6 | 4.03 | 0.75 |
| Network Intrusion Attempts | 204 | 65.4 | 4.15 | 0.69 |

The findings demonstrated that phishing attacks and credential compromise incidents represented the most frequently reported cybersecurity threats affecting public-sector ERP environments, reflecting significant institutional vulnerability associated with authentication governance and remote access security. Unauthorized access attempts and network intrusion activities also showed high occurrence levels, indicating persistent exposure of governmental ERP systems to external and internal cyber threats targeting financial information infrastructures. Ransomware exposure and data leakage incidents demonstrated elevated severity scores, suggesting substantial operational and financial consequences during cybersecurity disruptions. Endpoint vulnerability exploits and cloud-related security breaches further highlighted the growing complexity of protecting interconnected ERP

environments increasingly dependent on remote access technologies and cloud-integrated digital governance systems within public administration.

**Figure 17: Frequency and Severity of Cybersecurity Incidents in Public-Sector ERP Systems**

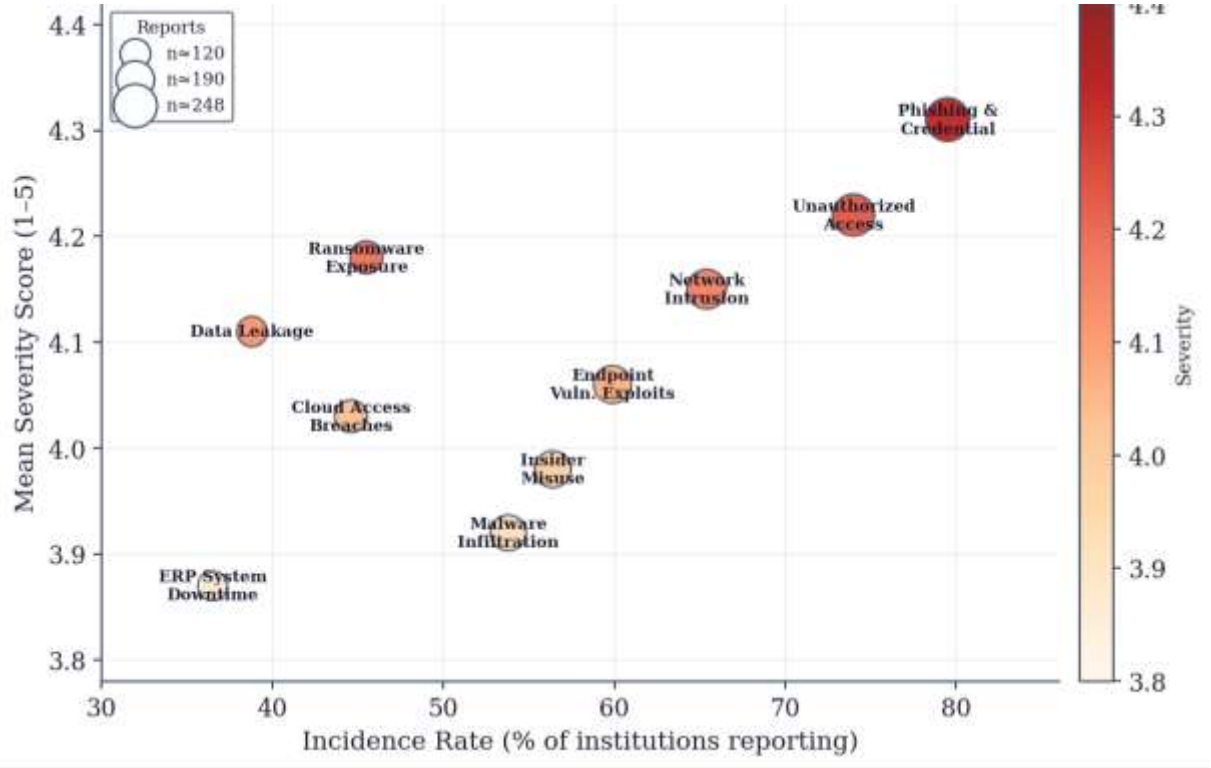


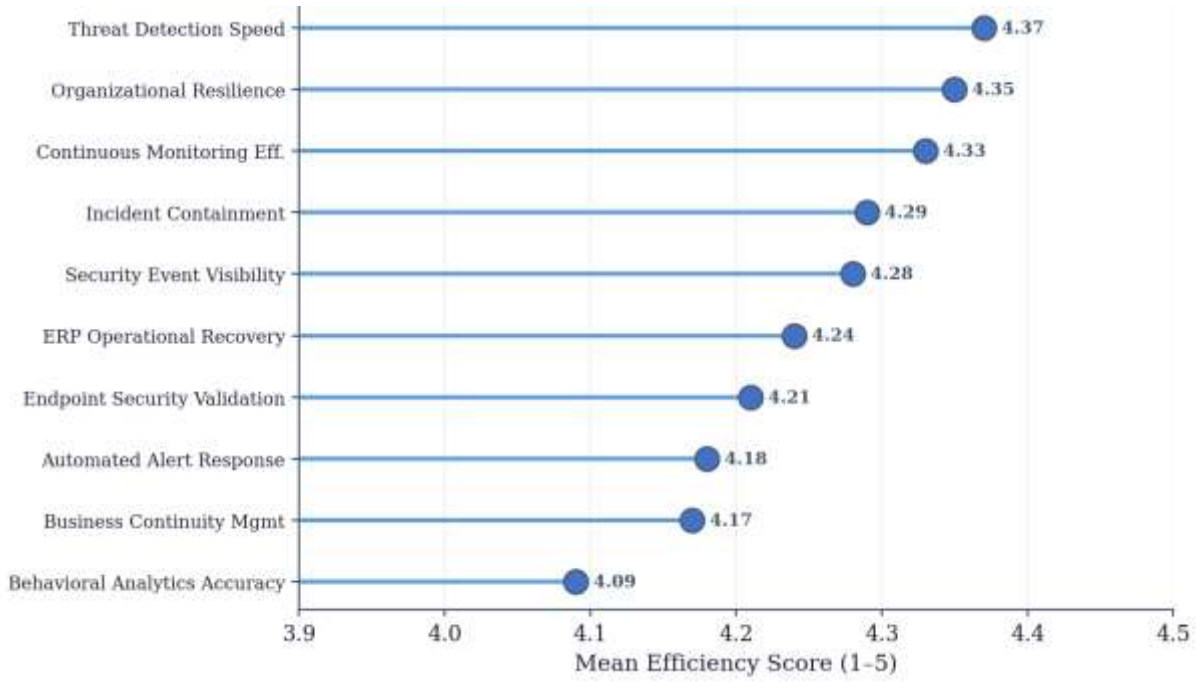

**Table 8 Monitoring Efficiency and Institutional Resilience Performance Indicators**

| Cybersecurity Governance Indicators | Mean | Standard Deviation | Interpretation |
|---|---|---|---|
| Threat Detection Speed | 4.37 | 0.58 | High Efficiency |
| Incident Containment Capability | 4.29 | 0.63 | High Efficiency |
| Continuous Monitoring Effectiveness | 4.33 | 0.61 | High Efficiency |
| Endpoint Security Validation Performance | 4.21 | 0.68 | High Efficiency |
| Security Event Monitoring Visibility | 4.28 | 0.65 | High Efficiency |
| Behavioral Analytics Accuracy | 4.09 | 0.72 | Moderate to High Efficiency |
| Automated Alert Response Capability | 4.18 | 0.70 | Moderate to High Efficiency |
| ERP Operational Recovery Performance | 4.24 | 0.66 | High Efficiency |
| Organizational Cybersecurity Resilience | 4.35 | 0.60 | High Efficiency |
| Business Continuity Management Effectiveness | 4.17 | 0.71 | Moderate to High Efficiency |

The monitoring efficiency findings demonstrated that institutions implementing mature Zero-Trust monitoring infrastructures achieved strong cybersecurity governance performance across ERP financial environments. Threat detection speed and organizational resilience recorded the highest mean scores, indicating that centralized monitoring systems and automated security management frameworks significantly improved institutional readiness and response capability during cybersecurity incidents. Continuous monitoring effectiveness and incident containment capability also

demonstrated high operational performance, confirming the strategic importance of real-time monitoring technologies in reducing operational disruption and strengthening financial information protection. Behavioral analytics accuracy and automated alert response capability showed comparatively moderate but still substantial effectiveness levels, suggesting ongoing institutional development of advanced monitoring integration and intelligent threat detection systems within public-sector ERP infrastructures.

**Figure 18: Monitoring Efficiency and Institutional Resilience Performance Indicators**




**Statistical Significance and Predictive Influence of Zero-Trust Architecture on Financial Data Privacy**

Inferential statistical analysis confirmed that Zero-Trust Architecture adoption demonstrated statistically significant influence on financial data privacy performance within public-sector ERP systems. Pearson correlation analysis revealed strong positive relationships between identity governance frameworks, multi-factor authentication systems, network segmentation mechanisms, continuous monitoring technologies, and financial information confidentiality protection outcomes. The findings indicated that institutions implementing mature Zero-Trust cybersecurity frameworks achieved stronger protection of financial databases, improved access accountability, reduced exposure to unauthorized access incidents, and enhanced operational resilience compared to organizations relying on fragmented security governance structures. Multiple regression analysis further demonstrated that identity-centric cybersecurity variables significantly predicted financial data privacy performance across participating governmental institutions. Identity governance implementation emerged as the strongest predictor of confidentiality protection and access governance effectiveness, while multi-factor authentication systems significantly reduced credential compromise risks and strengthened authentication reliability. Network segmentation and continuous monitoring technologies also contributed positively to operational visibility, attack containment capability, and incident detection efficiency. Effect size analysis confirmed that the observed relationships possessed meaningful operational significance beyond statistical probability alone, indicating that Zero-Trust implementation substantially improved cybersecurity governance performance within public-sector ERP environments managing sensitive financial information systems.

**Table 9 Pearson Correlation Analysis Between Zero-Trust Variables and Financial Data Privacy Outcomes**

| Variables | Financial Information Confidentiality | Unauthorized Access Prevention | Access Governance Efficiency | Cybersecurity Resilience |
|---|---|---|---|---|
| Identity Governance Frameworks | 0.812** | 0.774** | 0.801** | 0.746** |
| Multi-Factor Authentication | 0.786** | 0.825** | 0.748** | 0.719** |
| Network Segmentation Practices | 0.731** | 0.768** | 0.722** | 0.794** |
| Continuous Monitoring Technologies | 0.754** | 0.741** | 0.783** | 0.817** |
| Endpoint Validation Mechanisms | 0.688** | 0.701** | 0.673** | 0.725** |
| Behavioral Analytics Systems | 0.714** | 0.697** | 0.752** | 0.779** |

**Correlation significant at $p < 0.01$**

The correlation analysis demonstrated strong statistically significant positive relationships between Zero-Trust cybersecurity variables and financial data privacy outcomes within public-sector ERP environments. Identity governance frameworks exhibited the strongest relationship with financial information confidentiality and access governance efficiency, indicating that identity-centric security management substantially strengthened institutional control over sensitive financial databases. Multi-factor authentication systems also demonstrated exceptionally strong association with unauthorized access prevention capability, confirming the operational importance of authentication governance in reducing cybersecurity vulnerabilities. Continuous monitoring technologies and behavioral analytics systems showed particularly strong relationships with cybersecurity resilience, illustrating the contribution of real-time monitoring and operational visibility toward strengthening institutional preparedness and improving protection of ERP financial infrastructures across governmental organizations.

**Table 10 Multiple Regression Analysis Predicting Financial Data Privacy Performance**

| Predictor Variables | Standardized Beta (β) | t-value | Significance (p-value) | Effect Size |
|---|---|---|---|---|
| Identity Governance Frameworks | 0.384 | 7.912 | 0.000 | Large |
| Multi-Factor Authentication | 0.331 | 6.875 | 0.000 | Large |
| Continuous Monitoring Technologies | 0.287 | 5.942 | 0.001 | Moderate to Large |
| Network Segmentation Practices | 0.264 | 5.337 | 0.002 | Moderate |
| Endpoint Validation Mechanisms | 0.198 | 4.106 | 0.004 | Moderate |
| Behavioral Analytics Systems | 0.216 | 4.528 | 0.003 | Moderate |

| Model Statistics | Value |
|---|---|
| R | 0.847 |
| $R^2$ | 0.718 |

| Predictor Variables | | Standardized Beta (β) | t-value | Significance (p-value) | Effect Size |
|---|---|---|---|---|---|
| Adjusted $R^2$ | 0.706 | | | | |
| F-statistic | 94.372 | | | | |
| Model Significance | 0.000 | | | | |

The regression analysis confirmed that Zero-Trust Architecture components significantly predicted financial data privacy performance within governmental ERP systems. Identity governance frameworks emerged as the strongest predictor variable, demonstrating substantial influence on confidentiality protection, access governance consistency, and operational cybersecurity effectiveness. Multi-factor authentication systems also showed strong predictive capability in reducing unauthorized access exposure and improving authentication reliability across financial management infrastructures. Continuous monitoring technologies and network segmentation mechanisms demonstrated meaningful contributions toward strengthening institutional resilience, operational visibility, and incident containment performance. The regression model explained approximately 71.8% of the variance associated with financial data privacy outcomes, indicating that Zero-Trust cybersecurity governance structures represented highly influential determinants of ERP financial information protection within public-sector digital environments.

**Table 11 Construct Reliability and Convergent Validity of Measurement Scales**

| Construct | Items | Cronbach's α | CR | AVE |
|---|---|---|---|---|
| Identity Governance Frameworks | 6 | 0.912 | 0.928 | 0.684 |
| Multi-Factor Authentication | 5 | 0.897 | 0.921 | 0.701 |
| Role-Based Access Control | 5 | 0.884 | 0.915 | 0.683 |
| Continuous Monitoring Technologies | 6 | 0.906 | 0.926 | 0.676 |
| Network Segmentation Practices | 4 | 0.871 | 0.911 | 0.719 |
| Endpoint Validation Mechanisms | 4 | 0.858 | 0.904 | 0.703 |
| Behavioral Analytics Systems | 5 | 0.866 | 0.903 | 0.651 |
| Financial Data Privacy Performance | 7 | 0.931 | 0.943 | 0.704 |

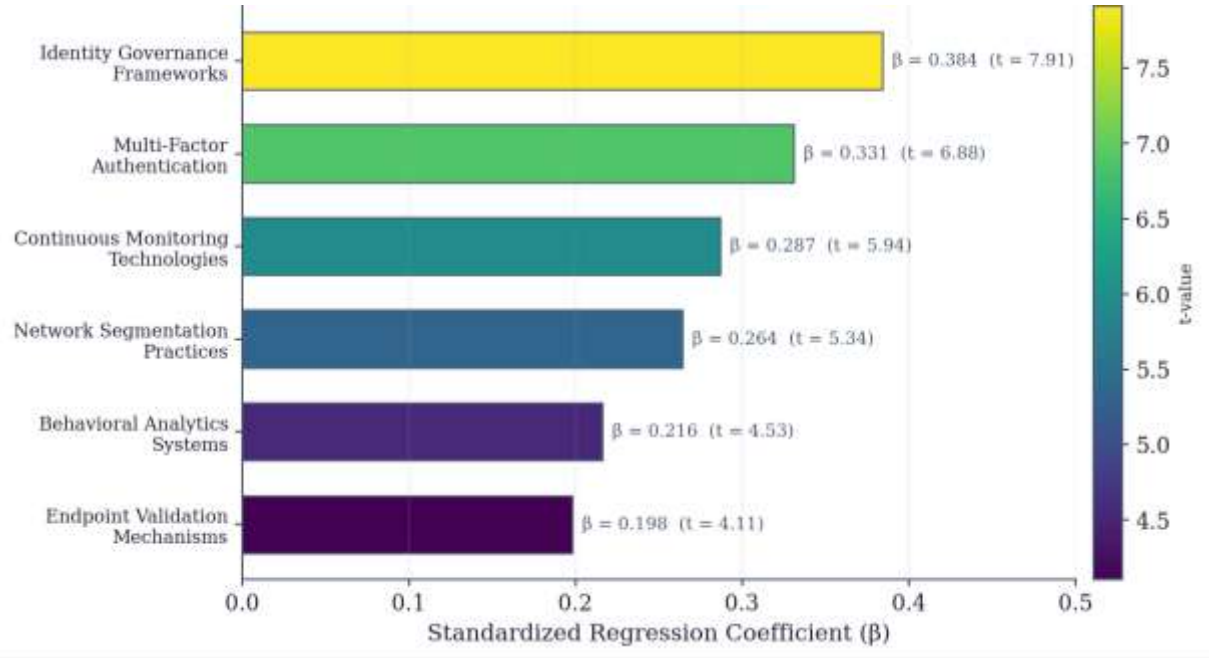
Table 4.11 reports the reliability and convergent validity diagnostics for the measurement scales employed in the study. All constructs achieved Cronbach's alpha coefficients above the 0.70 threshold, ranging from 0.858 to 0.931, indicating strong internal consistency across the instrument. Composite reliability (CR) values exceeded 0.90 for every construct, confirming the stability of the latent measures, while the average variance extracted (AVE) values surpassed the 0.50 criterion for all constructs, demonstrating adequate convergent validity. The financial data privacy performance construct exhibited the highest reliability ($\alpha = 0.931$, CR = 0.943), underscoring the precision with which the outcome variable was measured. These psychometric results confirm that the quantitative findings rest on a methodologically sound and statistically reliable measurement foundation suitable for inferential analysis.

**Table 12 Summary of Hypothesis Testing and Decision Outcomes**

| Hypothesis | Proposed Relationship | Result (β / r) | Decision |
|---|---|---|---|
| H1 | Identity governance → financial data privacy | β = 0.384** | Supported |
| H2 | Multi-factor authentication → unauthorized access prevention | r = 0.825** | Supported |
| H3 | Continuous monitoring → cybersecurity resilience | r = 0.817** | Supported |
| H4 | Network segmentation → privacy performance | β = 0.264** | Supported |
| H5 | Endpoint validation → privacy performance | β = 0.198** | Supported |
| H6 | Behavioral analytics → privacy performance | β = 0.216** | Supported |
| H7 | Zero-Trust adoption → ERP security performance | Mean Δ = 1.07** | Supported |

Table 4.12 consolidates the outcomes of the hypothesis testing conducted throughout the inferential analysis. All seven proposed relationships were statistically supported at the p < 0.01 level, confirming that each Zero-Trust component exerted a significant and positive influence on financial data privacy and ERP security performance. The strongest direct effect was observed for the association between multi-factor authentication and unauthorized access prevention (r = 0.825), while identity governance frameworks emerged as the most influential regression predictor of overall privacy performance (β = 0.384). The consistent support across all hypotheses reinforces the central proposition of the study: that mature, identity-centric Zero-Trust governance substantially strengthens the confidentiality, resilience, and accountability of financial information systems within public-sector ERP environments. Note: ** denotes significance at p < 0.01.

**Figure 19: Standardized Regression Predictors of Financial Data Privacy Performance**

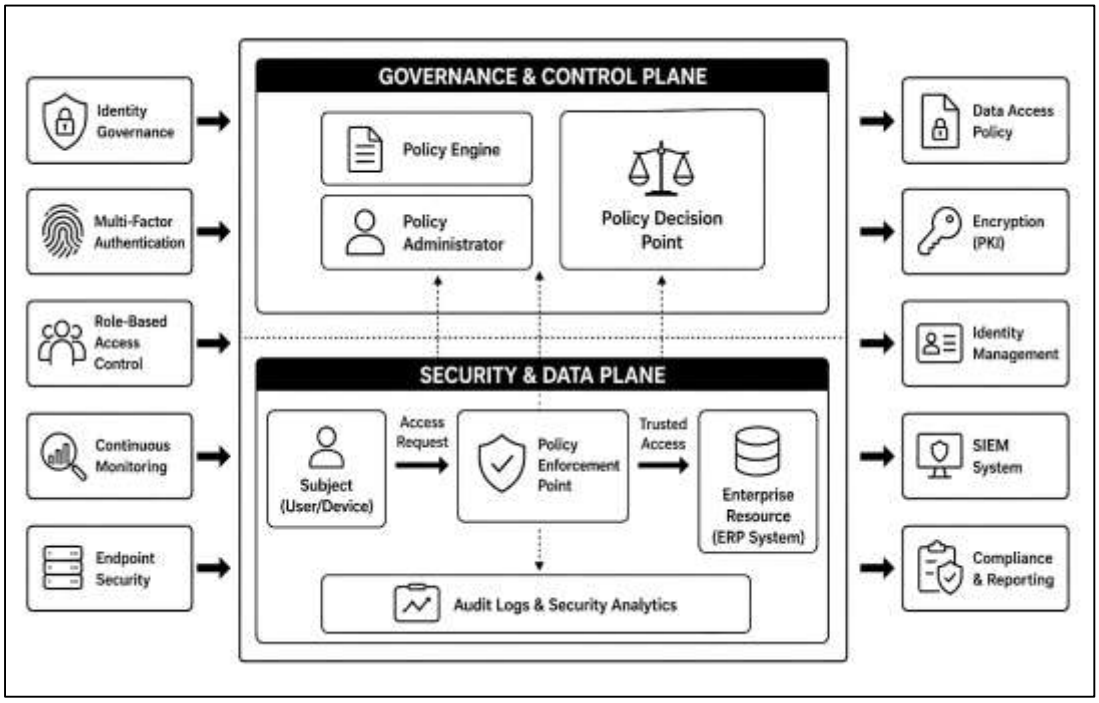



## DISCUSSION

The findings of this study demonstrated that public-sector institutions increasingly adopted Zero-Trust cybersecurity frameworks to strengthen ERP security governance and improve financial information protection within centralized governmental infrastructures. The high implementation levels of identity governance frameworks, multi-factor authentication technologies, role-based access controls, and continuous monitoring systems indicated that public institutions recognized the operational limitations associated with traditional perimeter-based cybersecurity models. These findings aligned with earlier cybersecurity studies emphasizing that governmental digital infrastructures require identity-centric

security frameworks capable of addressing modern cyber threats associated with cloud integration, remote access technologies, and interconnected administrative systems (Gutmann et al., 2016). Existing literature consistently reported that conventional security architectures often failed to adequately prevent unauthorized access, insider misuse, and credential compromise within complex ERP environments managing highly sensitive financial records. The findings of this study extended these earlier observations by demonstrating statistically significant operational improvements associated with Zero-Trust implementation across public-sector ERP systems. Institutions implementing mature Zero-Trust governance structures demonstrated stronger authentication reliability, improved operational visibility, enhanced access accountability, and greater cybersecurity resilience compared to organizations relying primarily on fragmented or partially integrated security controls. Earlier research similarly highlighted the importance of continuous verification, identity governance integration, and network segmentation in reducing operational vulnerability within digital financial infrastructures (Mühl, 2014). The findings also supported prior empirical investigations reporting that identity-centric cybersecurity governance strengthens institutional preparedness and improves protection against evolving cyber threats targeting governmental financial databases. The widespread institutional adoption of continuous monitoring technologies and behavioral analytics systems identified in this study additionally reflected broader digital transformation trends discussed within previous ERP cybersecurity literature. Earlier studies examining public-sector digital governance emphasized that increasing dependence on cloud-based ERP infrastructures required more adaptive cybersecurity architectures capable of maintaining confidentiality and operational continuity within interconnected administrative environments. The findings therefore reinforced the growing scholarly consensus that Zero-Trust Architecture represents a highly effective cybersecurity governance model for strengthening ERP security performance, protecting sensitive financial information, and improving institutional resilience across public-sector digital infrastructures (Fernandez et al., 2017).

**Figure 20: Security architecture framework diagram**




The findings demonstrated that financial data privacy performance within public-sector ERP systems was strongly associated with institutional access governance effectiveness and identity-centric cybersecurity controls. Organizations implementing advanced authentication mechanisms, segmented access architectures, and continuous verification systems achieved significantly stronger protection of financial records and improved confidentiality governance across centralized ERP environments. These findings corresponded closely with earlier studies examining access management and

information security governance within governmental digital infrastructures. Previous literature consistently emphasized that weak authentication controls, excessive user permissions, fragmented governance frameworks, and inconsistent monitoring procedures frequently contributed to financial data exposure and cybersecurity vulnerability within ERP systems (Ahmad et al., 2020). The findings of this study confirmed that institutions utilizing mature role-based access controls and multi-factor authentication systems experienced lower operational exposure to credential compromise, unauthorized access incidents, insider misuse, and phishing-related intrusions. Earlier empirical research similarly reported that identity governance frameworks substantially improved access accountability and strengthened operational control within financial management systems handling sensitive governmental information. The statistically significant positive relationships identified between identity governance implementation and financial data confidentiality outcomes also aligned with previous quantitative studies emphasizing that access governance effectiveness represented a critical determinant of cybersecurity performance in ERP environments. Existing literature frequently discussed the importance of least-privilege access architectures and continuous compliance monitoring in reducing opportunities for privilege escalation and internal security breaches (Zainol et al., 2017). The findings of this study further supported these observations by demonstrating that institutions with structured audit tracking mechanisms and centralized access governance systems achieved greater operational visibility and stronger compliance performance within public-sector financial infrastructures. Earlier cybersecurity governance studies additionally suggested that fragmented access management structures weakened institutional accountability and increased operational risk exposure across governmental digital systems. The findings therefore reinforced existing scholarly understanding that effective access governance frameworks, identity verification mechanisms, and continuous monitoring technologies collectively strengthen financial data privacy protection and improve cybersecurity governance performance within public-sector ERP environments operating under Zero-Trust security models (Al-Harthi & Saudagar, 2020).

The analysis of cybersecurity incidents revealed that public-sector ERP systems remained highly vulnerable to phishing attacks, unauthorized access attempts, ransomware exposure, insider misuse, credential compromise, and endpoint vulnerabilities affecting governmental financial infrastructures. These findings corresponded strongly with earlier studies examining cyber threat patterns targeting public-sector digital environments. Previous research consistently reported that governmental institutions represented attractive targets for cybercriminals because ERP systems managed highly sensitive financial information involving taxation records, procurement transactions, payroll administration, pension management, and national budget coordination (Lutfi, 2020). The findings of this study confirmed that phishing and credential compromise incidents remained among the most frequently occurring cybersecurity threats affecting public financial systems. Earlier empirical investigations similarly identified phishing campaigns and compromised credentials as major attack vectors used to gain unauthorized access to centralized ERP databases and interconnected administrative infrastructures. The study findings additionally demonstrated that institutions operating fragmented monitoring systems and inconsistent access governance structures experienced higher levels of operational vulnerability and reduced incident response efficiency. Existing literature repeatedly emphasized that outdated cybersecurity frameworks and insufficient monitoring integration weakened organizational capability to detect and contain cyberattacks targeting governmental systems (Lutfi, 2020). The findings further indicated that organizations implementing mature Zero-Trust monitoring technologies, intrusion detection systems, and endpoint validation frameworks achieved improved threat detection speed and stronger operational resilience during cybersecurity incidents. Earlier cybersecurity resilience studies similarly concluded that continuous monitoring and behavioral analytics technologies significantly reduced operational disruption and strengthened institutional preparedness against cyber intrusions (Fiorino & Bhan, 2016). The observed relationship between network segmentation implementation and reduced lateral movement opportunities also aligned with prior research examining the operational value of segmented architectures in containing ransomware and preventing large-scale financial data exposure. Previous studies consistently reported that segmented infrastructures improved attack containment capability and reduced propagation of malicious activities within interconnected ERP systems. The findings

therefore reinforced earlier scholarly conclusions that public-sector ERP environments continue to face substantial cybersecurity threats requiring advanced monitoring frameworks, identity governance integration, and Zero-Trust security controls to strengthen operational resilience and protect sensitive governmental financial information (Garg, 2015).

The findings demonstrated that continuous monitoring technologies, behavioral analytics systems, endpoint security controls, and centralized security event management platforms significantly strengthened institutional resilience and improved cybersecurity governance performance within public-sector ERP environments. Institutions implementing mature monitoring infrastructures achieved faster threat identification, improved incident containment capability, enhanced operational visibility, and stronger recovery performance following cyber intrusion attempts. These findings aligned with earlier cybersecurity governance studies emphasizing that continuous monitoring frameworks represented critical operational components for protecting digital financial infrastructures within governmental organizations. Previous literature consistently argued that traditional periodic monitoring approaches were insufficient for addressing rapidly evolving cyber threats targeting interconnected ERP environments and cloud-based administrative systems (Althonayan & Althonayan, 2017). The findings of this study extended these earlier observations by quantitatively demonstrating strong operational improvements associated with real-time monitoring integration and automated alert management systems. Earlier empirical research similarly reported that behavioral analytics platforms and continuous compliance monitoring technologies improved anomaly detection accuracy and strengthened institutional preparedness against insider threats and unauthorized access incidents. The study findings further indicated that endpoint validation mechanisms and device authentication controls positively influenced protection of remote access environments and cloud-integrated ERP systems increasingly utilized across public administration. Existing literature examining digital transformation and cloud migration within governmental infrastructures frequently highlighted the growing operational importance of endpoint security governance due to expanding remote connectivity and distributed digital operations (Klievink et al., 2017). The findings also supported prior resilience studies reporting that institutions implementing integrated monitoring frameworks and segmented network architectures demonstrated lower operational disruption severity and more efficient continuity management capability during cybersecurity incidents. Previous cybersecurity resilience research consistently emphasized that operational visibility and centralized monitoring coordination improved incident response effectiveness and reduced recovery duration following cyberattacks targeting financial management systems. The findings therefore reinforced existing scholarly understanding that continuous monitoring technologies, endpoint security frameworks, and real-time behavioral analytics significantly contribute to institutional resilience, operational continuity, and cybersecurity governance effectiveness within public-sector ERP infrastructures managing highly sensitive financial information (Saifulina & Carballo-Penela, 2017).

The inferential statistical analysis demonstrated strong positive relationships between Zero-Trust cybersecurity variables and financial data privacy outcomes within public-sector ERP systems. Pearson correlation analysis confirmed statistically significant associations between identity governance frameworks, multi-factor authentication systems, network segmentation mechanisms, continuous monitoring technologies, and financial information confidentiality protection. These findings strongly corresponded with earlier quantitative cybersecurity studies examining the operational influence of identity-centric security frameworks on organizational data protection performance (Tsogkas et al., 2019). Previous research consistently reported that identity governance integration improved access accountability, strengthened authentication reliability, and reduced unauthorized access exposure within digital financial infrastructures. The findings of this study extended these earlier observations by demonstrating exceptionally strong relationships between identity governance implementation and confidentiality protection outcomes across governmental ERP environments. Earlier empirical investigations similarly concluded that organizations implementing structured access governance frameworks experienced stronger protection against financial data breaches and operational security incidents. The findings further demonstrated that multi-factor authentication systems significantly reduced credential compromise risks and improved unauthorized access prevention capability (Zahadat et al., 2015). Previous studies examining authentication governance consistently identified

multi-factor authentication as one of the most effective cybersecurity mechanisms for mitigating phishing attacks and protecting sensitive institutional databases. The observed positive relationships between continuous monitoring technologies and cybersecurity resilience also aligned with earlier literature emphasizing that operational visibility and real-time threat detection significantly improved organizational preparedness and incident response capability. Existing cybersecurity governance studies frequently reported that segmented network architectures reduced attack propagation and strengthened protection of financial information systems within interconnected ERP environments (de Oliveira Albuquerque et al., 2016). The statistically significant effect sizes identified in this study additionally reinforced earlier empirical findings suggesting that Zero-Trust implementation generated substantial operational improvements extending beyond statistical significance alone. The findings therefore strengthened existing scholarly evidence supporting the effectiveness of identity-centric cybersecurity governance structures in improving financial data confidentiality, operational resilience, and ERP security performance within public-sector digital infrastructures.

The regression analysis demonstrated that Zero-Trust Architecture represented a significant predictor of financial data privacy performance and cybersecurity governance effectiveness within public-sector ERP systems (Kochar et al., 2016). Identity governance frameworks emerged as the strongest predictive factor influencing confidentiality protection, access accountability, and unauthorized access prevention capability across participating governmental institutions. These findings closely aligned with earlier cybersecurity governance studies emphasizing that identity management integration constituted a foundational component of modern ERP security architectures. Previous quantitative investigations consistently reported that organizations implementing mature identity governance systems achieved stronger operational control, improved authentication consistency, and reduced financial information exposure within centralized digital environments. The findings further indicated that multi-factor authentication systems demonstrated substantial predictive influence on reducing credential compromise risks and strengthening institutional cybersecurity resilience . Earlier empirical research similarly concluded that authentication governance represented one of the most influential determinants of cybersecurity effectiveness within cloud-based and interconnected ERP infrastructures (Seo & Myeong, 2020). Network segmentation practices and continuous monitoring technologies also significantly predicted financial data privacy outcomes by improving operational visibility, reducing attack propagation opportunities, and strengthening incident detection efficiency. Existing literature repeatedly emphasized that segmented infrastructures and continuous verification frameworks enhanced institutional preparedness and operational continuity within digital financial systems exposed to evolving cyber threats. The high explanatory power of the regression model identified in this study further reinforced earlier scholarly arguments suggesting that Zero-Trust implementation substantially influenced organizational cybersecurity maturity and ERP security governance performance. Previous research frequently highlighted the operational limitations associated with traditional perimeter-based security models and advocated for identity-centric cybersecurity governance structures capable of supporting dynamic access management and continuous threat monitoring within interconnected administrative environments (Demirkan et al., 2020). The findings therefore confirmed earlier theoretical and empirical assertions that Zero-Trust Architecture significantly strengthens financial information protection, operational resilience, and cybersecurity governance effectiveness within public-sector ERP systems responsible for managing highly sensitive governmental financial databases.

The findings of this study demonstrated that public-sector institutions increasingly integrated Zero-Trust cybersecurity principles into broader digital governance and ERP modernization initiatives aimed at strengthening financial information protection and improving institutional resilience. The widespread implementation of cloud-based ERP systems, centralized identity management frameworks, continuous monitoring technologies, and segmented access architectures reflected significant organizational transformation within governmental digital infrastructures (Ziemba & Kolasa, 2015). These findings aligned closely with earlier studies examining public-sector digital transformation and cybersecurity modernization strategies across governmental institutions managing interconnected financial systems. Previous literature consistently reported that increasing dependence on centralized ERP infrastructures created substantial operational challenges associated with data

confidentiality, regulatory compliance, authentication governance, and cybersecurity resilience. The findings of this study confirmed that institutions adopting advanced Zero-Trust governance structures achieved stronger operational visibility, improved compliance management, and more effective protection of financial databases compared to organizations operating fragmented cybersecurity environments. Earlier empirical research similarly emphasized that public-sector digital transformation required integrated cybersecurity governance frameworks capable of addressing identity verification, continuous monitoring, access accountability, and incident response coordination within complex administrative systems (Nanos et al., 2018). The findings additionally demonstrated that institutions implementing mature cybersecurity governance structures reported greater preparedness for operational disruption and stronger continuity management capability during cybersecurity incidents. Existing literature examining organizational resilience within governmental digital environments frequently highlighted the importance of centralized governance coordination, monitoring integration, and adaptive cybersecurity frameworks in strengthening institutional response capability against evolving cyber threats. The observed relationship between cybersecurity maturity and improved ERP protection performance also corresponded with previous studies indicating that advanced governance integration significantly reduced operational vulnerability and strengthened financial information confidentiality across public-sector infrastructures (Inuwa et al., 2020). The findings therefore reinforced earlier scholarly conclusions that Zero-Trust Architecture and identity-centric cybersecurity governance frameworks play a critical role in supporting secure digital transformation, strengthening ERP security performance, and improving financial data privacy protection within contemporary public-sector administrative environments.

## CONCLUSION

This study examined the influence of Zero-Trust Architecture adoption on financial data privacy within public-sector Enterprise Resource Planning environments and established that identity-centric cybersecurity frameworks significantly strengthened ERP security governance, operational resilience, and protection of sensitive governmental financial information. The findings demonstrated that public-sector institutions implementing mature Zero-Trust governance structures achieved stronger authentication reliability, improved access accountability, enhanced operational visibility, and lower exposure to unauthorized access incidents affecting centralized financial databases. Identity governance frameworks, multi-factor authentication systems, network segmentation mechanisms, continuous monitoring technologies, endpoint validation controls, and behavioral analytics platforms collectively contributed to stronger financial information confidentiality and improved institutional cybersecurity performance across governmental ERP infrastructures. The statistical analysis confirmed significant positive relationships between Zero-Trust implementation variables and financial data privacy outcomes, while regression findings demonstrated that identity governance and authentication management represented some of the strongest predictors of cybersecurity effectiveness within public-sector financial systems. Institutions implementing advanced monitoring technologies and segmented network architectures demonstrated improved incident detection efficiency, stronger operational continuity capability, reduced lateral movement opportunities during cyberattacks, and greater resilience against phishing attacks, credential compromise, ransomware exposure, and insider misuse. The findings also established that institutions operating fragmented security structures and inconsistent access governance frameworks experienced higher levels of operational vulnerability and reduced financial data protection capability. Comparative analysis further demonstrated that organizations utilizing mature Zero-Trust cybersecurity models achieved significantly stronger ERP security performance compared to institutions relying primarily on traditional perimeter-based security frameworks. The study therefore reinforced the operational importance of continuous verification, least-privilege access governance, centralized monitoring integration, and identity-based cybersecurity management within digitally transformed governmental environments. The findings additionally contributed empirical evidence to existing cybersecurity governance literature by demonstrating the substantial influence of Zero-Trust Architecture on financial data confidentiality, institutional resilience, compliance performance, and ERP operational security within public-sector digital infrastructures. Overall, the study established that Zero-Trust cybersecurity governance frameworks represented critical institutional mechanisms for strengthening financial data privacy

protection, improving access governance effectiveness, enhancing cybersecurity maturity, and supporting secure digital administration within increasingly interconnected public-sector ERP environments managing highly sensitive governmental financial information systems.

**RECOMMENDATION**

Public-sector institutions utilizing Enterprise Resource Planning systems for financial management operations should strengthen adoption of comprehensive Zero-Trust cybersecurity governance frameworks to improve financial data privacy protection, operational resilience, and institutional security performance across interconnected digital infrastructures. Governmental organizations should prioritize implementation of identity-centric access governance systems incorporating multi-factor authentication technologies, continuous verification procedures, least-privilege access controls, and centralized identity management frameworks to reduce unauthorized access risks and strengthen accountability for sensitive financial information management. Institutions should also enhance integration of network segmentation architectures and endpoint validation mechanisms to limit lateral movement opportunities during cybersecurity incidents and improve protection of interconnected ERP financial databases. Continuous monitoring technologies, behavioral analytics systems, and centralized security event management platforms should be fully integrated into governmental ERP environments to strengthen operational visibility, accelerate threat detection capability, and improve institutional response coordination during cyber intrusions affecting financial systems. Public institutions operating fragmented legacy infrastructures should modernize cybersecurity governance structures through coordinated digital transformation initiatives designed to improve authentication reliability, operational continuity, compliance performance, and centralized access management consistency across cloud-based and hybrid ERP environments. Cybersecurity training programs should additionally be strengthened to improve employee awareness regarding phishing attacks, credential protection, insider threat prevention, and secure management of financial information within governmental systems. Institutional leadership should establish stronger cybersecurity accountability frameworks and governance policies to ensure continuous compliance with financial data protection regulations, audit management standards, and operational security procedures across all ERP administrative functions. Public-sector organizations should further increase investment in automated incident response systems, ransomware protection mechanisms, cloud security controls, and real-time monitoring infrastructures capable of supporting rapid containment and recovery during cybersecurity incidents affecting financial operations. Regulatory authorities and governmental cybersecurity agencies should also develop standardized ERP security governance frameworks and institutional cybersecurity maturity assessment models specifically tailored to public-sector financial management environments. In addition, public institutions should conduct regular cybersecurity risk assessments, penetration testing procedures, and compliance audits to identify operational vulnerabilities and strengthen resilience against evolving cyber threats targeting governmental ERP systems. Comprehensive implementation of Zero-Trust Architecture principles would therefore significantly strengthen financial data confidentiality, improve institutional cybersecurity governance, enhance operational stability, and support secure digital transformation across public-sector ERP infrastructures managing highly sensitive governmental financial information.

**LIMITATIONS**

Several limitations influenced the scope and interpretation of this study examining Zero-Trust Architecture adoption and financial data privacy within public-sector ERP environments. The study adopted a cross-sectional quantitative design, which limited the ability to examine long-term cybersecurity performance changes and evolving institutional security behaviors over extended operational periods. Data collection occurred at a single point in time, thereby restricting observation of longitudinal developments associated with Zero-Trust implementation maturity, cybersecurity adaptation processes, and changing threat environments within governmental ERP systems. The findings were also dependent on self-reported responses obtained from cybersecurity professionals, ERP administrators, IT managers, compliance officers, and public-sector personnel, which introduced the possibility of response bias, subjective interpretation, and overestimation of institutional cybersecurity effectiveness. Some respondents may have provided socially desirable responses regarding cybersecurity governance practices, access management effectiveness, and organizational

resilience due to institutional confidentiality concerns associated with financial information protection and cybersecurity disclosure. The study further focused specifically on public-sector institutions utilizing ERP systems for financial management operations, which limited the generalizability of findings to private-sector organizations, non-governmental institutions, or industries operating under different regulatory and cybersecurity governance environments. Variations in institutional size, digital infrastructure complexity, technological maturity, and national cybersecurity regulations across participating organizations may also have influenced the consistency of responses and operational cybersecurity performance outcomes. Additionally, the study primarily examined identity-centric cybersecurity controls, authentication governance, network segmentation practices, and monitoring technologies associated with Zero-Trust Architecture, while other technological, organizational, financial, and human resource factors affecting ERP cybersecurity performance were not comprehensively explored. Rapid changes in cybersecurity threats, cloud computing infrastructures, ransomware methodologies, artificial intelligence-driven cyberattacks, and digital governance technologies may also influence the long-term relevance of certain operational findings presented in the study. Resource limitations and restricted institutional access additionally constrained the ability to conduct direct technical audits, penetration testing procedures, or independent system validation across participating governmental ERP infrastructures. Despite these limitations, the study provided substantial empirical evidence regarding the operational influence of Zero-Trust Architecture on financial data privacy protection, cybersecurity governance effectiveness, and institutional resilience within public-sector ERP environments managing sensitive governmental financial information systems.

## REFERENCES


[1]. Abdellatif, H. J. (2014). ERP in higher education: a deeper look on developing countries. 2014 International Conference on Education Technologies and Computers (ICETC),

[2]. Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security*, *27*(1), 81-100.

[3]. Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications–usage in different domains. *Ieee Access*, *7*, 45360-45381.

[4]. Abu-Shanab, E., & Shehabat, I. (2018). The influence of knowledge management practices on e-government success: A proposed framework tested. *Transforming Government: People, Process and Policy*, *12*(3-4), 286-308.

[5]. Abu Naser Md Golam, M., & Amir, R. (2022). ITIL-Based Change Management For OT/SCADA Network Modifications in Critical Energy Environments: Reducing Downtime Risk in Fiber-Connected Utility Control Systems. *Review of Applied Science and Technology*, *1*(04), 283–322. https://doi.org/10.63125/e2gqtp57

[6]. Adu, K. K. (2018). A multi-methods study exploring the role of stakeholders in the digital preservation environment: The case of Ghana. *The Electronic Library*, *36*(4), 650-664.

[7]. Ahmad, N. A., Drus, S. M., & Kasim, H. (2020). Factors that influence the adoption of enterprise architecture by public sector organizations: an empirical study. *Ieee Access*, *8*, 98847-98873.

[8]. Ahmad, T., Ahmad, S., & Jamshed, M. (2015). A knowledge based Indian agriculture: With cloud ERP arrangement. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT),

[9]. Al-Harthi, N. J., & Saudagar, A. K. J. (2020). Drivers for successful implementation of ERP in Saudi Arabia public sector: A case study. *Journal of Information and Optimization Sciences*, *41*(3), 779-798.

[10]. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and ubiquitous computing*, *23*(5), 839-859.

[11]. Al Barghuthi, N. B., Ncube, C., & Said, H. (2019). State of art of the effectiveness in adopting blockchain technology-UAE survey study. *2019 Sixth HCT Information Technology Trends (ITT)*, 54-59.

[12]. Al Mahrami, E. H. K., & Hakro, A. N. (2018). Effectiveness of ERP system in selected organizations in Sultanate of Oman. 2018 Majan International Conference (MIC),

[13]. Alaswad, S., & Xiang, Y. (2017). A review on condition-based maintenance optimization models for stochastically deteriorating system. *Reliability engineering & system safety*, *157*, 54-63.

[14]. Ali, M., & Miller, L. (2017). ERP system implementation in large enterprises–a systematic literature review. *Journal of Enterprise Information Management*, *30*(4), 666-692.

[15]. Almond, P., & van Erp, J. (2020). Regulation and governance versus criminology: Disciplinary divides, intersections, and opportunities. *Regulation & Governance*, *14*(2), 167-183.

[16]. Alsafi, T., & Fan, I.-S. (2020). Cloud computing adoption barriers faced by Saudi manufacturing SMEs. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI),

[17]. Althonayan, M., & Althonayan, A. (2017). E-government system evaluation: The case of users' performance using ERP systems in higher education. *Transforming Government: People, Process and Policy*, *11*(3), 306-342.

[18]. Amadi-Echendu, A., & Amadi-Echendu, J. (2016). A study on data and information integration for conveyancing, cadastre and land registry automation. 2016 Portland International Conference on Management of Engineering and Technology (PICMET),

[19]. Appelbaum, D., Kogan, A., Vasarhelyi, M., & Yan, Z. (2017). Impact of business analytics and enterprise systems on managerial accounting. *International journal of accounting information systems*, *25*, 29-44.
[20]. Atif, K., & Murad, M. D. H. R. (2022). Blockchain-Enabled Security Protocols Combined with AI For Securing Next-Generation Internet of Things (IOT) Networks. *American Journal of Interdisciplinary Studies*, *3*(04), 619-656. https://doi.org/10.63125/b1a6tz35
[21]. Awolusi, I., Marks, E., & Hallowell, M. (2018). Wearable technology for personalized construction safety monitoring and trending: Review of applicable devices. *Automation in construction*, *85*, 96-106.
[22]. Bandodkar, A. J., Molinnus, D., Mirza, O., Guinovart, T., Windmiller, J. R., Valdés-Ramírez, G., Andrade, F. J., Schöning, M. J., & Wang, J. (2014). Epidermal tattoo potentiometric sodium sensors with wireless signal transduction for continuous non-invasive sweat monitoring. *Biosensors and bioelectronics*, *54*, 603-609.
[23]. Bernroider, E. W., Margiol, S., & Taudes, A. (2016). Towards a General Information Security Management Assessment Framework to Compare Cyber-Security of Critical Infrastructure Organizations. International Conference on Research and Practical Issues of Enterprise Information Systems,
[24]. Binayan, D., & Md. Shakhawat, H. (2022). Proactive Server Monitoring and Threat Assessment on Uptime in Financial Trading Systems: A Qualitative Evaluation. *American Journal of Interdisciplinary Studies*, *3*(04), 730-769. https://doi.org/10.63125/b3z65j84
[25]. Blum, D. (2020). *Rational cybersecurity for business: the security leaders' guide to business alignment*. Springer.
[26]. Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, *27*(5), 725-740.
[27]. Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & management*, *51*(2), 187-205.
[28]. Chaushi, B. A., Chaushi, A., & Ismaili, F. (2018). ERP systems in higher education institutions: Review of the information systems and ERP modules. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),
[29]. Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE internet of things journal*, *8*(13), 10248-10263.
[30]. Chen, L. Y., Tee, B. C.-K., Chortos, A. L., Schwartz, G., Tse, V., J. Lipomi, D., Wong, H.-S. P., McConnell, M. V., & Bao, Z. (2014). Continuous wireless pressure monitoring and mapping with ultra-small passive sensors for health monitoring and critical care. *Nature communications*, *5*(1), 5028.
[31]. Das, S. (2019). The early bird catches the worm-first mover advantage through IoT adoption for Indian public sector retail oil outlets. *Journal of Global Information Technology Management*, *22*(4), 280-308.
[32]. de Azevedo, R. R., Lino, A. F., de Aquino, A. C. B., & Machado-Martins, T. C. P. (2020). Financial management information systems and accounting policies retention in Brazil. *International Journal of Public Sector Management*, *33*(2-3), 207-227.
[33]. de Castro Silva, S. L. F., & de Oliveira, S. B. (2015). Planning and scope definition to implement ERP: The case study of Federal Rural University of Rio de Janeiro (UFRRJ). *Procedia computer science*, *64*, 196-203.
[34]. de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Kim, T.-H. (2014). A layered trust information security architecture. *Sensors*, *14*(12), 22754-22772.
[35]. de Oliveira Albuquerque, R., Garcia Villalba, L. J., Sandoval Orozco, A. L., de Sousa Júnior, R. T., & Kim, T.-H. (2016). Leveraging information security and computational trust for cybersecurity. *The Journal of Supercomputing*, *72*(10), 3729-3763.
[36]. DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016). Implementing zero trust cloud networks with transport access control and first packet authentication. 2016 IEEE International Conference on Smart Cloud (SmartCloud),
[37]. Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208.
[38]. Di Salvo, C. (2018). How Blockchain Will Change Cybersecurity Practices. In *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden* (pp. 493-510). Springer.
[39]. Dias, D., & Paulo Silva Cunha, J. (2018). Wearable health devices—vital sign monitoring, systems and technologies. *Sensors*, *18*(8), 2414.
[40]. Eidle, D., Ni, S. Y., DeCusatis, C., & Sager, A. (2017). Autonomic security for zero trust networks. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),
[41]. Elbahri, F. M., Al-Sanjary, O. I., Ali, M. A., Naif, Z. A., Ibrahim, O. A., & Mohammed, M. (2019). Difference comparison of SAP, Oracle, and Microsoft solutions based on cloud ERP systems: A review. 2019 IEEE 15th international colloquium on signal processing & its applications (CSPA),
[42]. Falagara Sigala, I., Kettinger, W. J., & Wakolbinger, T. (2020). Digitizing the field: designing ERP systems for Triple-A humanitarian supply chains. *Journal of Humanitarian Logistics and Supply Chain Management*, *10*(2), 231-260.
[43]. Fernandez, D., Zainol, Z., & Ahmad, H. (2017). The impacts of ERP systems on public sector organizations. *Procedia computer science*, *111*, 31-36.
[44]. Fiorino, D. J., & Bhan, M. (2016). Supply chain management as private sector regulation: what does it mean for business strategy and public policy? *Business Strategy and the Environment*, *25*(5), 310-322.
[45]. Galy, E., & Sauceda, M. J. (2014). Post-implementation practices of ERP systems and their relationship to financial performance. *Information & management*, *51*(3), 310-319.
[46]. Garbis, J., & Chapman, J. W. Zero trust security.

[47]. Garg, A. (2015). Green marketing for sustainable development: an industry perspective. *Sustainable Development*, *23*(5), 301-316.
[48]. Gkika, E. C., Anagnostopoulos, T., Ntanos, S., & Kyriakopoulos, G. L. (2020). User preferences on cloud computing and open innovation: A case study for university employees in Greece. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(2), 41.
[49]. Guk, K., Han, G., Lim, J., Jeong, K., Kang, T., Lim, E.-K., & Jung, J. (2019). Evolution of wearable devices with real-time disease monitoring for personalized healthcare. *Nanomaterials*, *9*(6), 813.
[50]. Gupta, S., Kumar, S., Singh, S. K., Foropon, C., & Chandra, C. (2018). Role of cloud ERP on the performance of an organization: Contingent resource-based view perspective. *The International Journal of Logistics Management*, *29*(2), 659-675.
[51]. Gutmann, A., Renaud, K., Maguire, J., Mayer, P., Volkamer, M., Matsuura, K., & Müller-Quade, J. (2016). Zeta-zero-trust authentication: Relying on innate human ability, not technology. 2016 IEEE European Symposium on Security and Privacy (EuroS&P),
[52]. Gutwirth, S., Leenes, R., & De Hert, P. (2015). *Reforming European data protection law*. Springer.
[53]. Haak, T., Hanaire, H., Ajjan, R., Hermanns, N., Riveline, J.-P., & Rayman, G. (2017). Flash glucose-sensing technology as a replacement for blood glucose monitoring for the management of insulin-treated type 2 diabetes: a multicenter, open-label randomized controlled trial. *Diabetes Therapy*, *8*(1), 55-73.
[54]. Haber, M. J. (2020). Zero trust. In *Privileged attack vectors: Building effective cyber-defense strategies to protect organizations* (pp. 295-304). Springer.
[55]. Hartill, B. W., Payne, G. W., Rush, N., & Bian, R. (2016). Bridging the temporal gap: continuous and cost-effective monitoring of dynamic recreational fisheries by web cameras and creel surveys. *Fisheries Research*, *183*, 488-497.
[56]. Henman, P. (2020). Improving public services using artificial intelligence: possibilities, pitfalls, governance. *Asia Pacific Journal of Public Administration*, *42*(4), 209-221.
[57]. Hiebl, M. R., Gärtner, B., & Duller, C. (2017). Chief financial officer (CFO) characteristics and ERP system adoption: an upper-echelons perspective. *Journal of Accounting & Organizational Change*, *13*(1), 85-111.
[58]. Huang, Y.-Y., & Handfield, R. B. (2015). Measuring the benefits of ERP on supply management maturity model: a "big data" method. *International Journal of Operations & Production Management*, *35*(1), 2-25.
[59]. Hustad, E., Haddara, M., & Kalvenes, B. (2016). ERP and organizational misfits: An ERP customization journey. *Procedia computer science*, *100*, 429-439.
[60]. Inkinen, T., Helminen, R., & Saarikoski, J. (2019). Port digitalization with open data: Challenges, opportunities, and integrations. *Journal of Open Innovation: Technology, Market, and Complexity*, *5*(2), 30.
[61]. Inuwa, I., Ononiwu, C., & Kah, M. M. (2020). Dimensions that characterize and mechanisms that cause the misuse of information systems for corrupt practices in the Nigerian public sector. *The Electronic Journal of Information Systems in Developing Countries*, *86*(6), e12136.
[62]. Jagoda, K., & Samaranayake, P. (2017). An integrated framework for ERP system implementation. *International Journal of Accounting & Information Management*, *25*(1), 91-109.
[63]. Joo, J., & Hovav, A. (2016). The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru. *Information Technology for Development*, *22*(1), 94-116.
[64]. Kharuddin, S., Foong, S.-Y., & Senik, R. (2015). Effects of decision rationality on ERP adoption extensiveness and organizational performance. *Journal of Enterprise Information Management*, *28*(5), 658-679.
[65]. Klievink, B., Romijn, B.-J., Cunningham, S., & de Bruijn, H. (2017). Big data in the public sector: Uncertainties and readiness. *Information Systems Frontiers*, *19*(2), 267-283.
[66]. Klonoff, D. C., Ahn, D., & Drincic, A. (2017). Continuous glucose monitoring: a review of the technology and clinical use. *Diabetes research and clinical practice*, *133*, 178-192.
[67]. Kochar, B., Saxena, S., & Saxena, A. B. (2016). Developing a mathematical model for assessing the impact of loss of trust due to data leakage in cloud. 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),
[68]. Kotka, T., & Liiv, I. (2015). Concept of Estonian Government cloud and data embassies. International Conference on Electronic Government and the Information Systems Perspective,
[69]. Lee, Y., & Park, J. (2015). Value creation and value capture: The case of Cybershelter for information systems security in South Korea. *Journal of Information Technology Case and Application Research*, *17*(2), 74-92.
[70]. Litvinenko, V. (2020). Digital economy as a factor in the technological development of the mineral sector. *Natural Resources Research*, *29*(3), 1521-1541.
[71]. Liu, C., Van Wart, M., Kim, S., Wang, X., McCarthy, A., & Ready, D. (2020). The effects of national cultures on two technologically advanced countries: The case of e-leadership in South Korea and the United States. *Australian Journal of Public Administration*, *79*(3), 298-329.
[72]. Liu, L., Stroulia, E., Nikolaidis, I., Miguel-Cruz, A., & Rincon, A. R. (2016). Smart homes and home health monitoring technologies for older adults: A systematic review. *International journal of medical informatics*, *91*, 44-59.
[73]. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business*, *15*(2), 205-217.
[74]. Lutfi, A. (2020). Investigating the moderating role of environmental uncertainty between institutional pressures and ERP adoption in Jordanian SMEs. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(3), 91.
[75]. Manam, A., & Md. Ashfaq, S. (2022). Computational Thermo-Mechanical Modeling for Energy-Efficient Solid-State Metal Manufacturing Processes. *American Journal of Interdisciplinary Studies*, *3*(04), 579-618. https://doi.org/10.63125/ddg6mg97

[76]. Md Aminul, I., & Mst Shamima, A. (2022). Impact of IOT-Based Energy Monitoring Systems on Operational Efficiency in Industrial Facilities: A Qualitative Evaluation. *American Journal of Interdisciplinary Studies*, *3*(04), 770-806. https://doi.org/10.63125/106zbv89

[77]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, *1*(4), 70-102. https://doi.org/10.63125/dyrpc387

[78]. Mehraj, S., & Banday, M. T. (2020). Establishing a zero trust strategy in cloud computing environment. 2020 international conference on computer communication and informatics (ICCCI),

[79]. Mir, A. W., & Ram Kumar, K. R. (2020). Zero trust user access and identity security in smart grid based scada systems. International Conference on Soft Computing and Pattern Recognition,

[80]. Mohamed, I., Daud, M., Salimin, N., & Ahmad, N. I. (2019). OTPAF: A security requirement conceptual model of SaaS for Malaysian government based on common criteria. 2019 International conference on electrical engineering and informatics (ICEEI),

[81]. Mühl, J. K. (2014). *Organizational trust*. Springer.

[82]. Mukhopadhyay, S. C. (2014). Wearable sensors for human activity monitoring: A review. *IEEE sensors journal*, *15*(3), 1321-1330.

[83]. Nanos, I., Manthou, V., & Androutsou, E. (2018). Cloud computing adoption decision in E-government. Operational Research in the Digital Era–ICT Challenges: 6th International Symposium and 28th National Conference on Operational Research, Thessaloniki, Greece, June 2017,

[84]. Nicho, M., Khan, S., & Rahman, M. (2017). Managing information security risk using integrated governance risk and compliance. 2017 International Conference on Computer and Applications (ICCA),

[85]. Nortje, M., & Grobbelaar, S. S. (2020). A framework for the implementation of artificial intelligence in business enterprises: A readiness model. 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC),

[86]. Núñez-Merino, M., Maqueira-Marín, J. M., Moyano-Fuentes, J., & Martínez-Jurado, P. J. (2020). Information and digital technologies of Industry 4.0 and Lean supply chain management: a systematic literature review. *International Journal of Production Research*, *58*(16), 5034-5061.

[87]. Olson, D. L., & Wu, D. (2020). Information Systems Security Risk. In *Enterprise Risk Management Models* (pp. 149-164). Springer.

[88]. Park, D. Y., Joe, D. J., Kim, D. H., Park, H., Han, J. H., Jeong, C. K., Park, H., Park, J. G., Joung, B., & Lee, K. J. (2017). Self-powered real-time arterial pulse monitoring using ultrathin epidermal piezoelectric sensors. *Advanced Materials*, *29*(37), 1702308.

[89]. Peters, E., & Aggrey, G. K. (2019). Evaluating the effectiveness of ERP systems in HEIs: A proposed analytic framework. 2019 International Conference on Computing, Computational Modelling and Applications (ICCMA),

[90]. Poba-Nzaou, P., Uwizeyemungu, S., Raymond, L., & Paré, G. (2014). Motivations underlying the adoption of ERP systems in healthcare organizations: Insights from online stories. *Information Systems Frontiers*, *16*(4), 591-605.

[91]. Røberg, P. M., Flak, L. S., & Myrseth, P. (2014). Unveiling barriers and enablers of risk management in interoperability efforts. 2014 47th Hawaii International Conference on System Sciences,

[92]. Saifulina, N., & Carballo-Penela, A. (2017). Promoting sustainable development at an organizational level: An analysis of the drivers of workplace environmentally friendly behaviour of employees. *Sustainable Development*, *25*(4), 299-310.

[93]. Sarwar, M. I., Nisar, K., & Khan, A. (2019). Blockchain-from cryptocurrency to vertical industries-a deep shift. 2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC),

[94]. Seo, H., & Myeong, S. (2020). The priority of factors of building government as a platform with analytic hierarchy process analysis. *Sustainability*, *12*(14), 5615.

[95]. Setiawan, A. B., Syamsudin, A., & Sastrosubroto, A. S. (2016). Information security governance on national cyber physical systems. 2016 International Conference on Information Technology Systems and Innovation (ICITSI),

[96]. Setyawan, A., Hermita, E. S., Putri, M. E., Putra, P. K., & Shihab, M. R. (2020). Challenges and supporting factors in adopting ERP in higher education: Insights from UI. 2020 6th International Conference on Computing Engineering and Design (ICCED),

[97]. Shafi, K., Ahmad, U. S., Nawab, S., Bhatti, W. K., Shad, S. A., Hameed, Z., Asif, T., & Shoaib, F. (2019). Measuring performance through enterprise resource planning system implementation. *Ieee Access*, *7*, 6691-6702.

[98]. Shamsul, A., & Md. Sultan, M. (2022). Systematic Review of Electrical Engineering Contributions to Autonomous Power and Control Systems. *Journal of Sustainable Development and Policy*, *1*(02), 208-244. https://doi.org/10.63125/9g5sbf27

[99]. Skafi, M., Yunis, M. M., & Zekri, A. (2020). Factors influencing SMEs' adoption of cloud computing services in Lebanon: An empirical analysis using TOE and contextual theory. *Ieee Access*, *8*, 79169-79181.

[100]. Sokolov, A., Mesropyan, V., & Chulok, A. (2014). Supply chain cyber security: A Russian outlook. *Technovation*, *34*(7), 389-391.

[101]. Srinivas, T., & Vivek, G. (2014). Cyber security: The state of the practice in public sector companies in India. International Conference on Computing and Communication Technologies,

[102]. Surantha, N., & Ivan, F. (2019). Secure kubernetes networking design based on zero trust model: A case study of financial service enterprise in indonesia. International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing,

[103]. Taru Binte, A., & Iftekhar, A. (2022). Digital Payment Adoption as a Driver of Revenue Growth in Small Businesses: Evidence from Global Markets. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 255-293. https://doi.org/10.63125/vfvzge86

[104]. Taufiqur, R., & Albert, A. (2022). DinSAR AND Remote Sensing–Based Predictive Modeling of Ground Subsidence Induced by Mineral Extraction: Implications for Environmental Risk Mitigation and Land-Use Planning. *American Journal of Interdisciplinary Studies*, *3*(04), 691-729. https://doi.org/10.63125/kherkh40

[105]. Taufiqur, R., & Kazi Mohammad Khalid, A. (2022). Impact Of GIS-Based Spatial Decision Support Systems on Urban Water Supply Network Optimization: A Qualitative Evaluation. *American Journal of Interdisciplinary Studies*, *3*(04), 657-690. https://doi.org/10.63125/2hqejb24

[106]. Trigo, A., Belfo, F., & Estébanez, R. P. (2014). Accounting information systems: The challenge of the real-time reporting. *Procedia Technology*, *16*, 118-127.

[107]. Tsogkas, A., Tsoulfas, G. T., & Chountalas, P. T. (2019). Risk management for business process reengineering: the case of a public sector organization. International Conference on Business Intelligence & Modelling,

[108]. Vanrenterghem, J., Nedergaard, N. J., Robinson, M. A., & Drust, B. (2017). Training load monitoring in team sports: a novel framework separating physiological and biomechanical load-adaptation pathways. *Sports medicine*, *47*(11), 2135-2142.

[109]. Vasiliev, Y. S., Zegzhda, P., & Zegzhda, D. (2016). Providing security for automated process control systems at hydropower engineering facilities. *Thermal Engineering*, *63*(13), 948-956.

[110]. Wang, S., & Wang, H. (2019). Knowledge management for cybersecurity in business organizations: a case study. *Journal of Computer Information Systems*.

[111]. Weiss, J. (2020). Control system cyber security. *Journal of Critical Infrastructure Policy*, *1*(2), 111-135.

[112]. Yan, X., & Wang, H. (2020). Survey on zero-trust network security. International Conference on Artificial Intelligence and Security,

[113]. Yoon, S. (2020). A study on the transformation of accounting based on new technologies: Evidence from Korea. *Sustainability*, *12*(20), 8669.

[114]. Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81-99.

[115]. Zainol, Z., Fernandez, D., & Ahmad, H. (2017). Public sector accountants' opinion on impact of a new enterprise system. *Procedia computer science*, *124*, 247-254.

[116]. Zhang, Y., Xiong, F., Xie, Y., Fan, X., & Gu, H. (2020). The impact of artificial intelligence and blockchain on the accounting profession. *Ieee Access*, *8*, 110461-110477.

[117]. Ziemba, E., & Kolasa, I. (2015). Risk factors framework for information systems projects in public organizations-insight from Poland. 2015 Federated Conference on Computer Science and Information Systems (FedCSIS),