DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Haghighat, A., & Oyarhossein, S. (2027). The Impact of Digital Transformation and Cloud Computing on Security Challenges in IT Service Management. *Digital Transformation and Administration Innovation,* 5(4), 1-13.

Received date: 2026-08-02 Revised date: 2026-11-13 Accepted date: 2026-11-20 Initial Published date: 2026-11-25 Final Published date: 2027-07-01

The Impact of Digital Transformation and Cloud Computing on Security Challenges in IT Service Management

Abdullateef Haghighat[1], Shady Oyarhossein[1]*

1. Department of Information Technology Management, CT.C., Islamic Azad University, Tehran, Iran

*Correspondence: shady.oyarhossein@iau.ac.ir

Abstract

This study aimed to investigate the impact of digital transformation and cloud computing on security challenges in IT service management. This applied, quantitative, descriptive-correlational study was conducted among 384 managers, IT specialists, information security experts, cloud infrastructure professionals, and IT service management practitioners working in public and private organizations in Tehran, Iran. Participants were selected using a stratified purposive sampling approach based on professional involvement in digital transformation, cloud computing, information security, or IT service management. Data were collected using a structured questionnaire measuring digital transformation, cloud computing, and security challenges in IT service management. Content validity was evaluated through expert review, while construct validity and reliability were assessed using confirmatory measurement analysis, Cronbach's alpha, composite reliability, and average variance extracted. Data were analyzed using SPSS version 29 and SmartPLS version 4 through correlation analysis and partial least squares structural equation modeling. Bootstrapping with 5,000 resamples was used to assess the significance of structural paths. Digital transformation had a positive and statistically significant effect on security challenges in IT service management ($\beta = 0.26$, SE = 0.047, $t = 5.53$, $p < .001$). Cloud computing exerted a stronger positive effect on security challenges ($\beta = 0.40$, SE = 0.045, $t = 8.89$, $p < .001$). In addition, digital transformation had a strong positive effect on cloud computing adoption ($\beta = 0.61$, SE = 0.038, $t = 16.05$, $p < .001$). Digital transformation and cloud computing jointly explained 39% of the variance in security challenges in IT service management ($R^2 = 0.39$), and the model demonstrated predictive relevance ($Q^2 = 0.23$). The findings indicate that digital transformation and cloud computing significantly increase security complexity in IT service management, with cloud computing exerting the stronger direct effect; therefore, organizations should integrate cybersecurity governance, continuous monitoring, access control, configuration management, and resilience mechanisms into digital and cloud transformation initiatives.

Keywords: Digital Transformation; Cloud Computing; IT Service Management; Information Security; Cybersecurity

1. Introduction

Digital transformation has become one of the most consequential organizational developments affecting the design, delivery, governance, and security of information technology services. Organizations across public, private, educational, governmental, and commercial sectors increasingly rely on digitally integrated processes, cloud-based infrastructures, automated service platforms, artificial intelligence, advanced analytics, and interconnected information systems to improve operational efficiency and service responsiveness. Digital transformation, however, is not limited to the replacement of traditional technologies with

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

newer systems; rather, it involves the redesign of organizational processes, decision-making structures, service models, information flows, and technological capabilities around digital platforms and data-driven environments. The growing use of digital technologies has consequently changed the role of information technology from a supporting organizational function into a strategic infrastructure that directly influences continuity, competitiveness, service quality, innovation, and organizational resilience (Xu et al., 2023; Еремина et al., 2022). As digital technologies become embedded in core operations, organizations simultaneously become more dependent on the reliability, availability, integrity, and security of their IT service environments.

Information Technology Service Management (ITSM) provides the organizational and technical mechanisms through which IT services are planned, delivered, controlled, monitored, supported, and continuously improved. Contemporary ITSM approaches emphasize the alignment of IT capabilities with organizational objectives while ensuring service quality, availability, continuity, responsiveness, and value creation. Frameworks such as ITIL and ISO/IEC 20000 have been widely employed to structure service processes, clarify operational responsibilities, manage incidents and problems, improve service assets, and establish standardized approaches to IT governance and service delivery (Chege, 2024; Najoan & Mawuntu, 2023). The evolution of ITSM has increasingly moved beyond traditional service-desk operations toward enterprise-wide service management, integrated digital workflows, automation, predictive operations, and continuous service improvement (Maes, 2022; Mr, 2024). This transformation has increased the strategic importance of ITSM but has also expanded the range of risks that must be addressed within service management structures.

The expansion of digital transformation has intensified the complexity of contemporary IT service ecosystems. Digital services are increasingly dependent on interconnected applications, distributed databases, software interfaces, virtualized infrastructures, external service providers, mobile access, remote work environments, automated workflows, and continuously evolving software systems. These developments create broader attack surfaces and introduce new points of vulnerability that may not exist in traditional, centrally managed IT environments. The increasing integration of business processes with digital platforms also means that failures in cybersecurity, identity management, access control, configuration, or service continuity may have direct consequences for organizational performance. The growing convergence of governance, service management, quality assurance, and information security therefore requires organizations to adopt more integrated approaches to IT management (Sánchez et al., 2026). In such environments, the effectiveness of ITSM depends not only on process standardization and service quality but also on the organization's capacity to manage security threats across complex technological ecosystems.

Cloud computing represents one of the most significant technological foundations of contemporary digital transformation. By providing scalable, flexible, remotely accessible, and service-based computing resources, cloud environments enable organizations to reduce infrastructure constraints, increase operational flexibility, support digital innovation, and rapidly deploy new services. Organizations increasingly use software-as-a-service, platform-as-a-service, infrastructure-as-a-service, private clouds, public clouds, hybrid clouds, and multi-cloud environments to support business and IT operations. The migration of services to distributed cloud environments has substantially changed the architecture of IT service delivery, particularly because computing resources, applications, and data are increasingly located outside traditional organizational boundaries. This shift creates significant opportunities for agility and scalability, but it simultaneously increases concerns regarding visibility, access control, configuration management, data protection, third-party dependency, service availability, and accountability.

Cloud-enabled IT ecosystems are particularly vulnerable to configuration-related security problems. Misconfigured cloud resources, improperly maintained inventories, inaccurate configuration management databases, weak access policies, and insufficient monitoring can expose sensitive organizational resources to unauthorized access or service disruption. The implementation of cloud-based configuration management databases therefore requires careful attention to cybersecurity threats, asset relationships, infrastructure visibility, and configuration integrity (Dande, 2023). These challenges become more significant as organizations move toward hybrid environments in which cloud services must coexist with on-premise systems. Distributed cloud/on-premise ecosystems require resilient post-deployment architectures capable of supporting continuity, software evolution, system integration, and coordinated support across heterogeneous infrastructures (Cuellar-Fernandez et al., 2026). Consequently, cloud adoption does not merely change where IT resources are hosted; it changes the nature of IT service management and the security controls required to govern the entire service lifecycle.

**Copyright:** © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Another important consequence of digital transformation is the growing automation of IT operations. Modern organizations increasingly automate service requests, infrastructure provisioning, incident routing, configuration updates, monitoring, and routine operational tasks. Service automation can improve responsiveness, reduce manual workload, and support consistent service delivery, particularly in large-scale organizational environments (Rusdi et al., 2023). However, increasing automation also creates security and governance challenges because automated systems can execute actions at greater speed and scale than manual operations. Errors in automation logic, inappropriate permissions, inaccurate configuration data, or compromised credentials can therefore result in rapid propagation of operational failures or security incidents. This creates a need for stronger monitoring, policy enforcement, validation, and control mechanisms within ITSM processes.

The integration of DevOps practices into IT service environments has further accelerated the pace of software deployment and service change. DevOps emphasizes collaboration between development and operations teams, automation of software pipelines, continuous integration, continuous delivery, rapid feedback, and iterative improvement. These practices can significantly improve agility and service responsiveness, but they also require traditional ITSM processes to become more adaptive and closely integrated with development workflows (Faustino et al., 2025). Agile and ITIL-based approaches increasingly coexist in contemporary service environments, creating hybrid management models that seek to balance operational control with rapid technological change (Peliarachchi & Wijayanayake, 2023). This balance is particularly important from a security perspective because rapid deployment cycles can increase the likelihood that vulnerabilities, configuration errors, or insufficiently tested components are introduced into production environments.

The increasing use of artificial intelligence and advanced analytics is also reshaping ITSM. Artificial intelligence for IT operations, commonly referred to as AIOps, enables organizations to analyze large volumes of operational data, identify anomalies, automate incident detection, predict failures, and support intelligent decision-making in complex cloud-native environments (Tatineni, 2023). Predictive analytics similarly enables ITSM teams to anticipate service disruptions and identify operational patterns before they develop into major incidents (Familoni, 2024). Knowledge-based intelligent systems can further improve incident management by supporting classification, diagnosis, routing, and resolution of IT incidents within DevOps-oriented environments (Ahmed et al., 2023). More recent developments in agentic AIOps seek to extend these capabilities by developing systems that can autonomously analyze operational conditions, reason about potential responses, and execute actions with reduced human intervention (Zota & Constantinescu, 2025).

While such technologies can improve operational efficiency, they also increase the complexity of security governance. Automated decision-making systems may introduce new forms of dependency on algorithms, data quality, model behavior, and system integration. The adoption of generative artificial intelligence within enterprise ITSM environments further illustrates the growing relationship between digital transformation, service innovation, and organizational risk (Sharma et al., 2026). Generative AI can support knowledge retrieval, user interaction, incident resolution, documentation, and service-desk automation, but its implementation also requires careful consideration of access rights, confidential information, hallucinated outputs, model governance, and human oversight. Similarly, AI-supported training environments demonstrate the growing importance of digital simulation and adaptive technologies for preparing IT professionals to respond to complex service crises (Wong & Li, 2026). These developments reinforce the argument that digital maturity must be accompanied by equally mature security management practices.

Security management within ITSM also depends heavily on monitoring and observability. Modern IT environments generate large volumes of logs, alerts, performance indicators, and security events across applications, networks, infrastructure, and cloud services. Integrating monitoring tools is therefore essential for identifying incidents, correlating events, evaluating service performance, and detecting emerging operational problems (Cociorva et al., 2023). However, fragmented monitoring systems, incompatible tools, excessive alert volumes, and poor integration between operational and security platforms may reduce visibility rather than improve it. Effective ITSM increasingly requires unified monitoring architectures capable of combining operational data with security intelligence so that service continuity and cybersecurity can be managed as interconnected objectives rather than separate organizational functions.

The management of IT assets is another critical dimension of the relationship between digital transformation and security. Digital transformation increases the number and diversity of hardware, software, cloud resources, virtual assets, user identities,

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

endpoints, and third-party services that organizations must track and govern. Effective asset management supports service reliability by enabling organizations to understand the status, ownership, configuration, and lifecycle of technological resources. ITIL-based approaches have therefore been applied to improve IT asset management and strengthen the relationship between infrastructure control and service governance (Harjanto & Aji, 2024). In cloud-based environments, however, assets may be dynamically created, modified, or removed, making traditional inventory practices less effective. Poor asset visibility can create unknown vulnerabilities, unmonitored services, and unmanaged dependencies that increase organizational exposure to cyber threats.

The quality of ICT service management also depends on the institutional context in which services are provided. Studies of ICT service assessment have shown that structured ITSM frameworks can help organizations identify weaknesses in service delivery, infrastructure support, operational processes, and governance (Sukums et al., 2023). Similarly, ITSM intelligence models have been proposed to support complex digital government environments by integrating organizational, technological, and service-management capabilities (Nugroho et al., 2022). These perspectives are particularly relevant to public-sector and large organizational environments where digital transformation often occurs across multiple departments, legacy systems, user groups, and governance structures. Such complexity can amplify security challenges because organizations must simultaneously maintain continuity of legacy services while introducing new digital platforms and cloud-based technologies.

Security challenges are also closely related to data governance and secure access. Organizations increasingly manage sensitive information through shared platforms, remote environments, cloud repositories, and digital collaboration systems. Secure access environments have therefore become important mechanisms for allowing authorized users to work with sensitive data while maintaining confidentiality, governance, and controlled access (Samarage & Payne, 2025). The expansion of digital services increases the need for strong identity management, privileged access controls, encryption, authentication, auditability, and data-loss prevention. These requirements become more difficult to manage when data are distributed across multiple cloud providers, applications, and organizational boundaries. Consequently, the security responsibilities of ITSM teams increasingly extend beyond traditional infrastructure protection to include data governance, compliance, privacy, and third-party risk management.

A further challenge is the need for organizational agility without sacrificing security and service stability. Contemporary digital environments demand rapid adaptation to changing user requirements, technological innovation, emerging threats, and service disruptions. Systems thinking and technical agility have therefore become important for managing complex, dynamic technology environments in which multiple components and stakeholders are interdependent (Quilliam & Quilliam, 2026). From an ITSM perspective, agility requires the ability to introduce changes quickly while maintaining appropriate control over configuration, risk, continuity, security, and service performance. This creates a persistent tension between speed and governance. Excessively rigid controls may slow innovation, whereas insufficient controls may create vulnerabilities and operational instability.

The literature consequently suggests that digital transformation and cloud computing simultaneously improve organizational capability and increase security complexity. Digital transformation broadens the technological surface of the organization, increases interconnectivity, introduces new forms of automation, and accelerates the evolution of IT services. Cloud computing further distributes organizational resources across virtualized and externally managed infrastructures, making security governance more dependent on shared responsibility, third-party providers, configuration accuracy, and continuous monitoring. The resulting environment requires ITSM to integrate service quality, cybersecurity, resilience, automation, asset management, incident response, and governance within a unified management framework. Current research has examined these dimensions individually, including ITSM frameworks, cloud security, DevOps, AIOps, predictive analytics, service automation, asset management, and digital governance, but fewer studies have empirically examined the simultaneous effects of digital transformation and cloud computing on security challenges within IT service management environments.

This gap is particularly important because security challenges may not emerge solely from individual technologies but from the cumulative complexity created when organizations simultaneously digitalize processes, migrate services to cloud platforms, automate operations, adopt AI-supported tools, integrate heterogeneous systems, and rely on distributed service providers. Understanding these relationships is therefore necessary for developing more resilient ITSM structures capable of supporting digital innovation without increasing organizational vulnerability.

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Accordingly, the aim of this study was to investigate the impact of digital transformation and cloud computing on security challenges in IT service management.

2. Methods and Materials

This study employed an applied, quantitative, descriptive-correlational research design to investigate the impact of digital transformation and cloud computing on security challenges in IT service management. The research was conducted in Tehran, Iran, and the statistical population consisted of managers, supervisors, IT specialists, information security experts, cloud infrastructure specialists, and IT service management professionals employed in public and private organizations that had implemented digital transformation initiatives or used cloud-based information systems and services. To ensure that participants possessed sufficient professional familiarity with the research variables, eligibility criteria included having at least three years of professional experience in information technology, information security, cloud computing, digital transformation, or IT service management and direct involvement in the planning, implementation, supervision, support, or evaluation of organizational IT services. Individuals whose professional responsibilities were unrelated to digital technologies, cloud services, information security, or IT service processes were excluded from the study. A total of 384 participants were included in the final sample. This sample size was considered sufficient for multivariate statistical analysis and structural modeling and also provided adequate representation of professionals working in different organizational and technological environments in Tehran. Participants were selected using a stratified purposive sampling approach. First, organizations using cloud infrastructures, digital platforms, integrated information systems, or formal IT service management practices were identified, and participants were subsequently recruited from relevant IT, information security, digital transformation, infrastructure, and service management units. Efforts were made to achieve adequate variation in organizational type, occupational position, professional experience, and area of technical expertise. Participation was voluntary, and respondents were informed about the purpose of the study, the confidentiality of their responses, and their right to withdraw from the research process at any stage. Questionnaires with substantial missing data or inconsistent response patterns were excluded before the final statistical analysis.

Data were collected using a structured questionnaire developed on the basis of the theoretical literature concerning digital transformation, cloud computing, information security, cybersecurity risk, and IT service management. The instrument consisted of four main sections. The first section collected demographic and occupational information, including age, gender, educational level, years of professional experience, organizational sector, occupational position, and field of IT specialization. The second section measured digital transformation through items related to digital strategy, organizational digitalization, process automation, integration of digital technologies, data-driven decision-making, digital service innovation, employee digital capabilities, and the extent to which digital technologies had been incorporated into organizational processes and IT service delivery. The third section assessed cloud computing through dimensions including the degree of cloud service adoption, use of software, platform, and infrastructure services, scalability, service accessibility, resource virtualization, interoperability, migration of organizational systems to cloud environments, dependency on cloud service providers, and the integration of cloud solutions with organizational IT infrastructure. The fourth section evaluated security challenges in IT service management and included items addressing confidentiality, integrity, availability, identity and access management, data leakage, unauthorized access, cyberattacks, service disruption, cloud misconfiguration, third-party risks, compliance requirements, incident response, vulnerability management, business continuity, security monitoring, and the protection of IT services throughout their operational lifecycle.

All substantive items were measured using a five-point Likert scale ranging from 1, indicating strongly disagree, to 5, indicating strongly agree. Higher scores for the digital transformation and cloud computing constructs represented greater implementation and organizational adoption, whereas higher scores for security challenges reflected a greater perceived level of security-related complexity, vulnerability, and risk within IT service management processes. The initial questionnaire was reviewed by a panel of university faculty members and experienced professionals in information technology management, information security, cloud computing, and IT service management to assess the relevance, clarity, comprehensiveness, and conceptual appropriateness of the items. Based on their comments, ambiguous expressions were revised, repetitive items were removed, and several statements were modified to better reflect the organizational context of IT service delivery. Content validity was subsequently assessed through expert judgment, and the final instrument was considered to provide adequate

**Copyright:** © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

coverage of the study constructs. A pilot administration was also conducted with a small group of IT professionals who were not included in the final sample to evaluate item comprehensibility and preliminary reliability. Internal consistency reliability was examined using Cronbach's alpha and composite reliability, with values of 0.70 or higher considered acceptable. Construct validity was assessed through confirmatory factor analysis by examining standardized factor loadings, average variance extracted, composite reliability, and discriminant validity. An average variance extracted value of at least 0.50 and a composite reliability value greater than 0.70 were considered evidence of satisfactory convergent validity and construct reliability.

Data analysis was performed using SPSS version 29 and SmartPLS version 4. Before hypothesis testing, the dataset was screened for incomplete responses, extreme values, inconsistent response patterns, and potential data-entry errors. Descriptive statistics, including frequency, percentage, mean, and standard deviation, were calculated to summarize the demographic characteristics of the participants and the distribution of the principal study variables. The distributional characteristics of the quantitative variables were examined using skewness and kurtosis indices, and multicollinearity among the predictor variables was assessed using tolerance and variance inflation factor statistics. Correlation analysis was initially conducted to determine the direction and strength of the relationships among digital transformation, cloud computing, and security challenges in IT service management.

The measurement model was subsequently evaluated using partial least squares structural equation modeling. Indicator reliability was examined through standardized outer loadings, while internal consistency was assessed using Cronbach's alpha and composite reliability. Convergent validity was evaluated using the average variance extracted, and discriminant validity was investigated using the Fornell-Larcker criterion and the heterotrait-monotrait ratio. After confirmation of the adequacy of the measurement model, the structural model was examined to evaluate the proposed relationships among the study variables. Standardized path coefficients were estimated to determine the magnitude and direction of the effects of digital transformation and cloud computing on security challenges in IT service management. The statistical significance of the structural paths was assessed using a bootstrapping procedure with 5,000 resamples. Coefficients of determination were used to evaluate the proportion of variance in the dependent variable explained by the predictor constructs, and effect size and predictive relevance indices were examined to assess the explanatory and predictive strength of the model. Statistical significance was evaluated at the 0.05 level, and all coefficients were interpreted in relation to both their statistical significance and practical magnitude.

3. Findings and Results

A total of 384 valid questionnaires were included in the final statistical analysis. Of the respondents, 238 participants (62.0%) were male and 146 (38.0%) were female. Regarding age, 67 participants (17.4%) were younger than 30 years, 151 (39.3%) were between 30 and 39 years, 112 (29.2%) were between 40 and 49 years, and 54 (14.1%) were 50 years of age or older. In terms of educational attainment, 74 respondents (19.3%) held a bachelor's degree, 225 (58.6%) held a master's degree, and 85 (22.1%) held a doctoral degree or an equivalent professional qualification. Professional experience was also relatively diverse: 69 participants (18.0%) had between 3 and 5 years of experience, 117 (30.5%) had between 6 and 10 years, 122 (31.8%) had between 11 and 15 years, and 76 (19.8%) had more than 15 years of professional experience. With regard to occupational specialization, 106 respondents (27.6%) worked primarily in IT service management, 91 (23.7%) in information security or cybersecurity, 72 (18.8%) in cloud infrastructure and systems administration, 65 (16.9%) in digital transformation or enterprise systems, and 50 (13.0%) in other closely related IT management functions. Furthermore, 219 participants (57.0%) were employed in private-sector organizations and 165 (43.0%) in public or government-affiliated organizations. These characteristics indicated that the sample represented a relatively experienced and professionally diverse group of IT specialists with direct exposure to digital transformation, cloud computing, and security-related aspects of IT service management.

Table 1. Descriptive Statistics and Correlations among the Main Study Variables

Variable	Mean	SD	Skewness	Kurtosis	1	2	3
Digital Transformation	3.78	0.64	-0.42	0.31	1.00		
Cloud Computing	3.69	0.67	-0.35	0.27	0.61***	1.00	
Security Challenges in IT Service Management	3.57	0.71	-0.18	-0.09	0.48***	0.56***	1.00

As shown in Table 1, the mean score for digital transformation was 3.78 (SD = 0.64), indicating that the organizations represented in the sample had generally progressed beyond the initial stages of digitalization and had incorporated digital

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

technologies into a substantial proportion of their organizational and IT service processes. Cloud computing obtained a mean score of 3.69 (SD = 0.67), suggesting a relatively high level of adoption of cloud-based infrastructures, platforms, applications, and related service models. The mean score for security challenges in IT service management was 3.57 (SD = 0.71), demonstrating that respondents perceived security-related difficulties as a considerable issue within digitally transformed and cloud-enabled IT service environments. The skewness values ranged from -0.42 to -0.18, while kurtosis values ranged from -0.09 to 0.31, indicating no substantial deviation from normality at the univariate level. The correlation analysis showed a positive and statistically significant relationship between digital transformation and cloud computing ($r = 0.61$, $p < .001$). Digital transformation was also positively related to security challenges in IT service management ($r = 0.48$, $p < .001$), while cloud computing showed an even stronger positive association with security challenges ($r = 0.56$, $p < .001$). These results provided preliminary support for the assumption that greater organizational dependence on digital and cloud-based technologies is associated with a more complex security environment and greater exposure to security-related challenges in the management and delivery of IT services.

Table 2. Measurement Model Assessment: Reliability and Convergent Validity

Construct	Number of Items	Factor Loading Range	Cronbach's Alpha	Composite Reliability	AVE
Digital Transformation	8	0.71–0.86	0.89	0.92	0.59
Cloud Computing	8	0.70–0.88	0.91	0.93	0.62
Security Challenges in IT Service Management	10	0.72–0.87	0.92	0.94	0.60

The results presented in Table 2 confirm the satisfactory reliability and convergent validity of the measurement model. Standardized factor loadings for digital transformation ranged from 0.71 to 0.86, those for cloud computing ranged from 0.70 to 0.88, and those for security challenges in IT service management ranged from 0.72 to 0.87. All retained indicators therefore exceeded the commonly accepted minimum loading threshold of 0.70, demonstrating adequate indicator reliability. Cronbach's alpha coefficients were 0.89 for digital transformation, 0.91 for cloud computing, and 0.92 for security challenges in IT service management, showing a high degree of internal consistency among the indicators associated with each latent construct. Composite reliability values ranged from 0.92 to 0.94 and were also well above the minimum acceptable threshold of 0.70. The average variance extracted values were 0.59 for digital transformation, 0.62 for cloud computing, and 0.60 for security challenges, all exceeding the recommended value of 0.50. This finding demonstrates that each latent construct explained more than half of the variance in its respective indicators and supports the convergent validity of the measurement model. Collectively, the reliability and validity statistics indicated that the measurement scales were sufficiently consistent and conceptually coherent for subsequent evaluation of the structural relationships among the study variables.

Table 3. Discriminant Validity and Multicollinearity Assessment

Construct	Digital Transformation	Cloud Computing	Security Challenges	VIF Range
Digital Transformation	0.768			1.58–2.41
Cloud Computing	0.61	0.787		1.64–2.53
Security Challenges in IT Service Management	0.48	0.56	0.775	1.71–2.66

Table 3 presents the results of the discriminant validity and multicollinearity assessments. The square root of the AVE was 0.768 for digital transformation, 0.787 for cloud computing, and 0.775 for security challenges in IT service management. In every case, the square root of the AVE exceeded the correlations between the corresponding construct and the other latent variables, satisfying the Fornell-Larcker criterion and demonstrating adequate discriminant validity. Specifically, the correlation between digital transformation and cloud computing was 0.61, while the correlations of digital transformation and cloud computing with security challenges were 0.48 and 0.56, respectively. These values were lower than the square root of the AVE for the relevant constructs, indicating that each construct shared more variance with its own indicators than with other constructs in the model. The variance inflation factor values ranged from 1.58 to 2.66 across all indicators and predictor constructs. Because all VIF values were substantially below the conservative threshold of 5.00, and also below the more restrictive threshold of approximately 3.00 in most cases, there was no evidence of problematic multicollinearity. These results indicate that digital transformation and cloud computing, although conceptually and empirically related, represented sufficiently distinct organizational capabilities and could therefore be included simultaneously as predictors of security challenges in IT service management without causing unstable parameter estimates.

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Table 4. Structural Model Results for the Effects of Digital Transformation and Cloud Computing on Security Challenges in IT Service Management

Structural Path	β	SE	t	p	f^2	Result
Digital Transformation → Security Challenges	0.26	0.047	5.53	< .001	0.08	Supported
Cloud Computing → Security Challenges	0.40	0.045	8.89	< .001	0.19	Supported
Digital Transformation → Cloud Computing	0.61	0.038	16.05	< .001	0.59	Supported

As reported in Table 4, both digital transformation and cloud computing exerted statistically significant positive effects on security challenges in IT service management. The direct effect of digital transformation on security challenges was positive and significant (β = 0.26, SE = 0.047, t = 5.53, p < .001), indicating that greater organizational progress toward digital transformation was associated with increased security complexity in the management of IT services. The corresponding effect size was $f^2 = 0.08$, representing a small-to-moderate practical contribution. Cloud computing demonstrated a stronger direct effect on security challenges (β = 0.40, SE = 0.045, t = 8.89, p < .001), with an effect size of $f^2 = 0.19$, indicating a moderate contribution to the explanation of security-related challenges. These results suggest that extensive dependence on shared computing resources, remote service delivery, virtualization, third-party cloud providers, distributed data storage, and externally managed infrastructures substantially increases the need for advanced security governance within IT service management processes. In addition, digital transformation had a strong positive effect on cloud computing adoption (β = 0.61, SE = 0.038, t = 16.05, p < .001), with a relatively large effect size of $f^2 = 0.59$. This finding shows that organizations with more developed digital transformation strategies were considerably more likely to rely on cloud-based infrastructures and services. Together, digital transformation and cloud computing explained 39% of the variance in security challenges in IT service management ($R^2 = 0.39$; adjusted $R^2 = 0.39$), demonstrating moderate explanatory power. The Stone-Geisser predictive relevance coefficient for security challenges was $Q^2 = 0.23$, which was greater than zero and therefore confirmed the predictive relevance of the structural model. Overall, the structural results demonstrated that cloud computing represented the stronger immediate predictor of security challenges, whereas digital transformation contributed both directly to security complexity and indirectly by promoting greater organizational dependence on cloud-based service architectures.

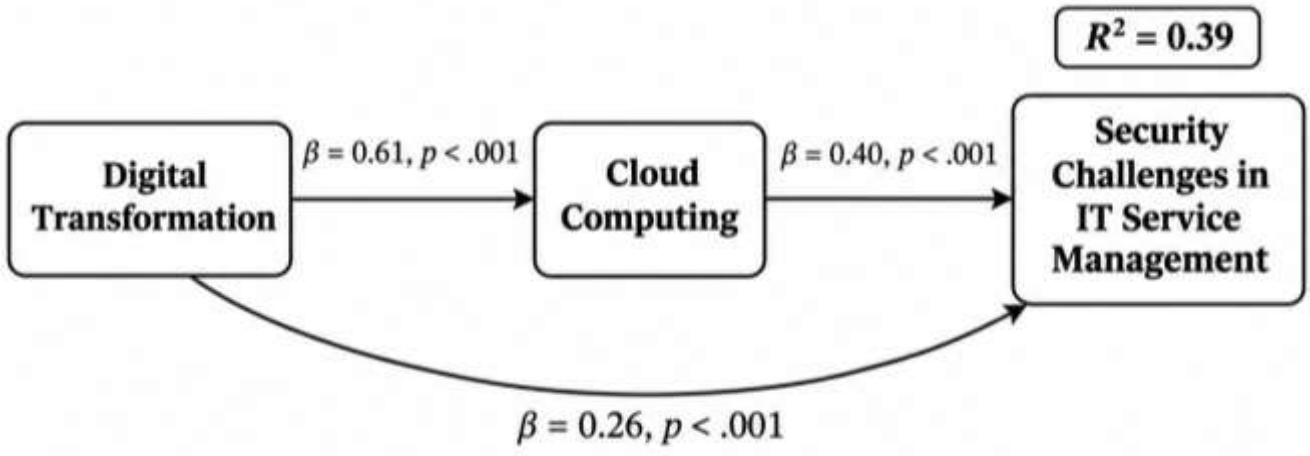

Figure 1. Structural Model of the Effects of Digital Transformation and Cloud Computing on Security Challenges in IT Service Management

The structural model illustrated in Figure 1 summarizes the pattern of relationships among the principal constructs investigated in the study. Digital transformation exerted a significant direct effect on security challenges in IT service management (β = 0.26, p < .001) while simultaneously demonstrating a strong positive relationship with cloud computing adoption (β = 0.61, p < .001). Cloud computing, in turn, had the strongest direct effect on security challenges (β = 0.40, p < .001). The pattern of coefficients suggests that security challenges are not attributable to a single technological factor but emerge from the interaction between broader organizational digitalization and increasing dependence on distributed cloud environments. As organizations transform traditional business and service processes into digitally integrated operations, their IT service environments become increasingly interconnected, automated, data-intensive, and dependent on external or hybrid infrastructures. This development expands the number of technological interfaces, identities, applications, data repositories,

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

network connections, and third-party relationships that must be secured. At the same time, adoption of cloud computing changes traditional security boundaries because organizational resources are no longer confined to internally controlled infrastructure. The significant paths shown in the model therefore demonstrate that both digital transformation and cloud computing contribute to the growth of security complexity, although cloud computing represents the more substantial immediate source of security challenges within IT service management. The model's R^2 value of 0.39 further indicates that these two technological factors together account for a meaningful proportion of variation in perceived security challenges and provide a substantial empirical basis for interpreting the security implications of contemporary digital service environments.

4. Discussion and Conclusion

The present study examined the effects of digital transformation and cloud computing on security challenges in IT service management and produced several important findings. First, digital transformation had a positive and statistically significant effect on security challenges in IT service management ($\beta = 0.26$, $p < .001$). Second, cloud computing exerted an even stronger positive effect on security challenges ($\beta = 0.40$, $p < .001$). Third, digital transformation had a strong positive effect on cloud computing adoption ($\beta = 0.61$, $p < .001$). Together, digital transformation and cloud computing explained 39% of the variance in security challenges in IT service management, indicating that the two variables represent substantial determinants of the security complexity experienced in contemporary IT service environments. These findings support the view that technological modernization does not merely generate operational efficiencies and service improvements; it also alters the structure of organizational risk, expands the number of technological dependencies that must be controlled, and increases the managerial burden associated with maintaining confidentiality, integrity, availability, continuity, access control, and secure service delivery.

The significant positive effect of digital transformation on security challenges can be explained by the increasingly pervasive role of digital technologies in organizational processes. Digital transformation generally involves the integration of digital platforms, data-driven systems, automation, interconnected applications, remote access mechanisms, and intelligent technologies into core organizational activities. As the digital footprint of an organization expands, the number of assets, interfaces, user identities, endpoints, databases, workflows, and external connections that require protection also increases. This interpretation is consistent with the broader literature emphasizing that digitalization changes the architecture of organizational information systems and consequently increases demands for governance, monitoring, and security control (Xu et al., 2023; Еремина et al., 2022). The finding is also compatible with research showing that IT governance, service management, and quality assurance must increasingly be treated as interconnected domains rather than isolated managerial functions (Sánchez et al., 2026). Therefore, the observed relationship between digital transformation and security challenges appears to reflect the broader transformation of IT from a bounded technical support function into a distributed organizational infrastructure.

The positive relationship between digital transformation and security challenges is also consistent with evidence regarding the evolution of ITSM itself. Traditional ITSM focused heavily on standardized service processes, incident handling, configuration control, and service quality, whereas contemporary ITSM increasingly operates in highly dynamic environments characterized by automation, agile delivery, artificial intelligence, and continuous change. Studies of ITSM practice indicate that mature service management requires coordinated processes, governance, and clear operational responsibilities (Chege, 2024; Maes, 2022). At the same time, modern service-management platforms increasingly incorporate digital workflows and automation capabilities that extend ITSM beyond conventional service-desk functions (Mr, 2024). The present findings reinforce this literature by showing that greater digitalization is accompanied by greater perceived security complexity. In practical terms, organizations that intensify digital transformation may face a growing need to synchronize service management with cybersecurity governance, risk management, data protection, and business continuity mechanisms.

The stronger effect of cloud computing on security challenges is particularly noteworthy. The standardized path coefficient for cloud computing was 0.40, which exceeded the direct effect of digital transformation. This suggests that cloud adoption may represent a more immediate source of security complexity than digital transformation in general. The result can be explained by the architectural characteristics of cloud computing. Cloud environments distribute applications, data, infrastructure, and services beyond traditional organizational boundaries and frequently involve shared responsibility between

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

the client organization and external service providers. As a result, security management must address identity and access management, third-party risk, multi-tenancy, remote administration, misconfiguration, data location, service continuity, API security, and dependency on cloud vendors. Dande's analysis of cloud configuration management database implementation similarly highlights the cybersecurity risks associated with cloud configuration, asset relationships, and infrastructure visibility (Dande, 2023). The present study therefore supports the view that cloud computing transforms the nature of security governance rather than merely relocating computing resources.

The findings are also aligned with research on hybrid and distributed cloud environments. Cuellar-Fernandez et al. argue that post-deployment continuity in distributed cloud/on-premise ecosystems requires resilient architectures that can coordinate heterogeneous infrastructures and evolving software environments (Cuellar-Fernandez et al., 2026). This perspective helps explain why cloud computing emerged as the strongest direct predictor of security challenges in the current study. When organizations operate across public cloud, private cloud, hybrid infrastructure, legacy systems, and distributed applications, the security boundary becomes more fragmented. Responsibility for service continuity, patching, monitoring, access control, and configuration becomes distributed across multiple technological and organizational actors. Such fragmentation can increase the likelihood of gaps in accountability, inconsistent controls, and delayed responses to emerging threats. Therefore, the stronger effect of cloud computing is theoretically and operationally plausible.

The results also correspond with studies emphasizing the importance of monitoring and observability in complex IT environments. Cociorva et al. demonstrated that integrated monitoring tools play an essential role in evaluating performance and supporting operational awareness across technology environments (Cociorva et al., 2023). In cloud-based and digitally transformed organizations, the volume and variety of operational data increase substantially. Security teams and ITSM units must therefore process logs, alerts, configuration changes, service-health indicators, network events, and incident data from multiple systems. When these monitoring mechanisms are fragmented or poorly integrated, organizations may experience reduced visibility, slower incident detection, and difficulty distinguishing operational failures from security incidents. The current findings can therefore be interpreted as evidence that the expansion of digital and cloud services increases not only the attack surface but also the complexity of maintaining adequate situational awareness.

The strong positive effect of digital transformation on cloud computing adoption ($\beta = 0.61$, $p < .001$) further clarifies the interdependence between the two technological developments. Digital transformation often requires scalable infrastructure, flexible service provisioning, remote accessibility, rapid deployment, and integration across applications and organizational units, all of which are facilitated by cloud computing. The result is consistent with contemporary digital architectures in which cloud services function as an enabling platform for broader transformation initiatives. As organizations automate processes and digitalize services, cloud infrastructure provides the elasticity and scalability needed to support these developments. This relationship can also be understood in light of service automation research showing that digitally enabled organizations increasingly rely on automated provisioning and scalable service models to improve efficiency and responsiveness (Rusdi et al., 2023). Therefore, the present result suggests that cloud computing should not be treated as an isolated technical choice, but rather as a core infrastructure through which digital transformation is operationalized.

The relationship between digital transformation, cloud computing, and security challenges can also be interpreted through the growing integration of DevOps and agile practices within ITSM. DevOps accelerates software deployment, increases automation, and integrates development and operational activities, thereby improving responsiveness but also increasing the frequency and velocity of change. Faustino et al. reported that DevOps significantly affects IT service management and alters established approaches to service delivery and control (Faustino et al., 2025). Likewise, Peliarachchi and Wijayanayake emphasized the growing convergence between ITIL and agile approaches in managing software and IT operations (Peliarachchi & Wijayanayake, 2023). These studies support the current findings because rapid and continuous change can create additional security challenges if governance, testing, access control, and configuration processes do not evolve at the same pace. In other words, digital transformation creates a dynamic environment in which traditional security controls may become insufficient unless they are embedded directly into automated service and development processes.

The findings are also consistent with the increasing role of artificial intelligence and advanced analytics in IT operations. Tatineni described AIOps as an important mechanism for supporting cloud-native DevOps and improving IT operations management through artificial intelligence (Tatineni, 2023). Familoni similarly emphasized the role of predictive analytics in

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

enhancing service quality by anticipating incidents and performance issues (Familoni, 2024). Ahmed et al. showed that knowledge-based intelligent systems can support IT incident management in DevOps environments (Ahmed et al., 2023). These studies align with the present results because the growing use of AI-supported ITSM systems increases the sophistication of service management while simultaneously introducing new security and governance requirements. The more organizations depend on automated predictions and machine-assisted decisions, the more they must ensure the integrity of data, model behavior, system permissions, and automated responses.

Recent developments in generative AI further reinforce this argument. Sharma et al. demonstrated that enterprise implementation of generative AI can enhance IT service management but also requires careful organizational integration and governance (Sharma et al., 2026). Similarly, Zota and Constantinescu proposed agentic AIOps frameworks that extend automation toward more autonomous operational decision-making (Zota & Constantinescu, 2025). These technologies may improve incident response, knowledge retrieval, and service-desk efficiency, but they can also increase risk if automated agents operate with excessive privileges, incomplete context, or inadequate human supervision. Wong and Li's work on AI-supported simulations of IT support crises further illustrates how AI is becoming embedded in both operational and training contexts (Wong & Li, 2026). The present findings therefore suggest that security challenges will likely intensify as digital transformation becomes increasingly AI-enabled, especially in cloud environments where automation can operate across large and distributed infrastructures.

The importance of asset management also provides further support for the observed relationships. Harjanto and Aji showed that ITIL-based approaches can improve IT asset management by strengthening control over technological resources (Harjanto & Aji, 2024). However, digital transformation and cloud computing complicate asset management because virtual machines, containers, cloud resources, software services, and identities can be created and removed dynamically. In such environments, incomplete inventories and inaccurate configuration records can generate hidden security exposures. This interpretation corresponds with Dande's emphasis on the cybersecurity implications of cloud CMDB implementation (Dande, 2023). The present findings suggest that the security consequences of digital transformation and cloud adoption may partly arise from the difficulty of maintaining accurate and continuously updated visibility over complex technological assets.

The explanatory power of the structural model is also meaningful. Digital transformation and cloud computing accounted for 39% of the variance in security challenges, while the predictive relevance value was positive. This indicates that the model captured a substantial portion of the factors shaping perceived security complexity. At the same time, the remaining unexplained variance indicates that other variables are also important. These may include cybersecurity maturity, organizational culture, regulatory requirements, employee competence, governance quality, vendor dependency, incident-response capability, IT budget, and management support. Studies conducted in institutional and public-sector contexts have emphasized the importance of structured ICT service assessment and management maturity in achieving reliable service outcomes (Nugroho et al., 2022; Sukums et al., 2023). Consequently, the effect of technological transformation on security should be interpreted within the broader organizational environment in which IT services are managed.

The results also have implications for secure access and data governance. Samarage and Payne emphasized the importance of secure access environments for supporting the use of sensitive information while maintaining appropriate controls (Samarage & Payne, 2025). This concern becomes particularly relevant as digital transformation expands the movement of data across cloud services, remote platforms, and integrated applications. The current findings suggest that stronger adoption of digital and cloud technologies may increase challenges related to authentication, authorization, privileged access, data leakage, and compliance. Therefore, organizations should view data governance and identity management as core ITSM responsibilities rather than separate cybersecurity functions.

Finally, the findings support the broader argument that agility and resilience must be managed simultaneously. Quilliam and Quilliam emphasized the importance of technical agility and systems thinking in complex technology environments (Quilliam & Quilliam, 2026). The present study extends this perspective by showing that greater technological agility may also generate additional security complexity. Organizations therefore face a dual requirement: they must remain sufficiently flexible to innovate and adapt while maintaining robust control over service continuity, infrastructure, access, configuration, and risk. The


Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

practical challenge is not to reduce digitalization or cloud adoption, but to ensure that security capabilities evolve proportionally with technological change.

One limitation of this study is that it employed a cross-sectional design, which restricts the ability to establish causal relationships over time. The data were also collected from professionals working in Tehran, which may limit the generalizability of the findings to organizations operating in other regions or countries with different technological, regulatory, economic, and organizational conditions. In addition, the study relied on self-reported questionnaire data, which may be influenced by respondents' perceptions, organizational experiences, or social desirability. Although the measurement model demonstrated satisfactory reliability and validity, the constructs represented broad organizational phenomena and may not capture all technical dimensions of digital transformation, cloud computing, and cybersecurity. The model also focused on two major predictors and therefore did not include potentially important contextual variables such as organizational size, cybersecurity maturity, governance structure, regulatory compliance, outsourcing intensity, or management support.

Future research should examine the relationships identified in this study using longitudinal designs in order to determine how security challenges evolve as organizations progress through different stages of digital transformation and cloud adoption. Comparative studies across industries, regions, and countries could clarify whether the magnitude of the observed effects differs according to regulatory environments, organizational maturity, or technological infrastructure. Future models could also incorporate mediating or moderating variables such as cybersecurity maturity, IT governance quality, organizational resilience, employee competence, digital culture, third-party dependency, and security investment. Researchers may additionally distinguish between public, private, hybrid, and multi-cloud environments and examine specific security outcomes such as incident frequency, data breaches, service downtime, configuration errors, and response effectiveness. Mixed-method and case-study approaches could provide deeper insight into the mechanisms through which digital and cloud transformation generate security complexity in real organizational settings.

For practice, organizations should integrate cybersecurity directly into digital transformation and cloud adoption strategies rather than treating security as a separate or subsequent function. IT service management processes should be redesigned to include continuous risk assessment, automated security monitoring, identity and access governance, configuration control, asset visibility, incident-response integration, and third-party risk management. Organizations should ensure that cloud responsibilities are clearly defined between internal teams and service providers, particularly for access management, data protection, backup, logging, patching, and incident handling. Security controls should also be embedded into DevOps, automation, and AI-enabled workflows so that rapid service delivery does not weaken governance. Regular training should be provided for ITSM, cloud, and security personnel, while executive management should ensure that security capability grows proportionally with the scale of digital transformation. Continuous auditing, resilience testing, and cross-functional coordination between IT operations, cybersecurity, development, and business units can further reduce the risks associated with increasingly complex digital service environments.

Ethical Considerations

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

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

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

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

References

Ahmed, S., Singh, M., Ramlan, E. I., Harkin, K., Bucholc, M., & Coyle, D. (2023). Knowledge-Based Intelligent System for IT Incident DevOps. 1-7. https://doi.org/10.1109/aiops59134.2023.00005

Chege, S. M. (2024). IT Service Management System Practices in Kenya. *The International Journal of Management Science and Business Administration*, *10*(3), 47-64. https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.103.1003

Cociorva, A., Onofrei, N., & Vîlcea, A.-L. (2023). Tool Integrations for Monitoring Solutions and Associated Performance Analysis. *Proceedings of the International Conference on Business Excellence*, *17*(1), 1929-1943. https://doi.org/10.2478/picbe-2023-0170

Cuellar-Fernandez, R., Chaname-Salazar, J., & Cornejo, J. (2026). Engineering-Resilient Post-Deployment Lifecycle Dynamics: A Technical Analysis of IT Support Architectures for System Continuity and Software Evolution in Distributed Cloud/on-Premise Computing ERP Ecosystems. *Information*, *17*(10), 947. https://doi.org/10.3390/info17100947

Dande, F. (2023). Enterprise Service Management Cybersecurity Threats: Exploring Cloud Configuration Management Database (CMDB) Implementation Within Community Colleges. https://doi.org/10.46254/na8.20230157

Familoni, B. T. (2024). Theoretical Perspectives on Predictive Analytics in It Service Management: Enhancing Service Quality. *International Journal of Frontiers in Engineering and Technology Research*, *6*(1), 040-048. https://doi.org/10.53294/ijfetr.2024.6.1.0028

Faustino, J. ã., Pereira, R., Silva, M. M. d., Adriano, D., & Camargo, V. C. B. (2025). The Impact of DevOps in IT Service Management. *Journal of Global Information Management*, *33*(1), 1-49. https://doi.org/10.4018/jgim.392902

Harjanto, A., & Aji, R. F. (2024). Improving IT Assets Management With ITIL 4 Framework. *Jurnal Ilmu Komputer Dan Informasi*, *17*(2), 127-143. https://doi.org/10.21609/jiki.v17i2.1195

Maes, S. H. (2022). ITSM and ESM in the Bigger World. Separation of Concerns: A Modern Approach of ITIL for the Enterprise. https://doi.org/10.31219/osf.io/ugr3p

Mr, S. (2024). A Comprehensive Survey on ServiceNow for IT Service Management. *International Journal of Scientific Research in Engineering and Management*, *08*(05), 1-5. https://doi.org/10.55041/ijsrem35395

Najoan, H. K., & Mawuntu, D. J. (2023). Establish and Implement PAM and PRM ISO 20000-1:2011. *Brilliance Research of Artificial Intelligence*, *3*(2), 359-368. https://doi.org/10.47709/brilliance.v3i2.3296

Nugroho, H., Aradea, A., & Surendro, K. (2022). IT Service Management Intelligence Model to Support the Implementation of Electronic Government System (EGS) in Indonesia. *International Journal on Advanced Science Engineering and Information Technology*, *12*(2), 494-500. https://doi.org/10.18517/ijaseit.12.2.13789

Peliarachchi, A., & Wijayanayake, J. I. (2023). A-Itil, ITIL and Agile Based Advanced Framework for Managing Software and IT Related Bau: A Systematic Literature Review. *Journal of Desk Research Review and Analysis*, *1*(1), 84-97. https://doi.org/10.4038/jdrra.v1i1.8

Quilliam, G., & Quilliam, A. (2026). Technical Agility and Systems Thinking in the Delivery of Military Simulation Training. *Simulation & Gaming*, *57*(5), 696-721. https://doi.org/10.1177/10468781261437540

Rusdi, A., Hardian, B., Raharjo, T., & Simanugkalit, T. (2023). Service Automation Implementation for Delivering CaaS at the Ministry of Finance of Indonesia. *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(5), 1174-1181. https://doi.org/10.29207/resti.v7i5.5032

Samarage, C. R., & Payne, A. A. (2025). The Melbourne Institute Data Lab, a Secure Access Environment for Informing Future Social and Economic Policy. *Australian Economic Review*, *58*(3), 259-271. https://doi.org/10.1111/1467-8462.70018

Sánchez, A. Q., Rodríguez, J. R. G., Chaires, L. A. F., Arceo-Olague, J. G., Rodríguez-Abdalá, V. I., & Sandoval-Aréchiga, R. (2026). Mapping IT Reference Frameworks for Governance, Service Management, and Quality Assurance: A Scoping Review. *Information*, *17*(8), 807. https://doi.org/10.3390/info17080807

Sharma, A. J., Rathore, B., Biswas, B. N., Xiao, X., & Gupta, R. (2026). Generative <scp>AI</Scp> Implementation in Enterprises: Lessons From a Case Study of Enhanced <scp>IT</Scp> Service Management. *Information Systems Journal*, *36*(5), 661-690. https://doi.org/10.1111/isj.70029

Sukums, F. K., Kisenge, R. R., & Wamala-Larsson, C. (2023). Assessment of ICT Services Using the Information Technology Infrastructure Library Framework at Muhimbili University of Health and Allied Sciences, Tanzania. *East African Journal of Science Technology and Innovation*, *4*(3). https://doi.org/10.37425/eajsti.v4i3.643

Tatineni, S. (2023). AIOps in Cloud-Native DevOps: IT Operations Management With Artificial Intelligence. *Journal of Artificial Intelligence & Cloud Computing*, *2*(1), 1. https://doi.org/10.47363/jaicc/2023(2)154

Wong, J. M. S., & Li, K.-c. (2026). Digital Frontline: An AI Role-Play Simulation of IT Support Crises in the Implementation of Agile-Blended Learning. *Digital*, *6*(2), 36. https://doi.org/10.3390/digital6020036

Xu, X., Wang, X., Zhang, Y., Yue, Y., & Wu, Y. (2023). ICT Framework for the Personal Learning Environment (PLE-ICT) in Higher Education: Results From Experts' Interview. https://doi.org/10.3233/faia230166

Zota, R. D., & Constantinescu, R. (2025). A Practical Approach to Defining a Framework for Developing an Agentic AIOps System. *Electronics*, *14*(9), 1775. https://doi.org/10.3390/electronics14091775

Еремина, И. А., Тарабукина, Т. В., & Oblizov, A. (2022). The Use of Digital Technologies to Improve the Information Support of Agricultural Enterprises. *International Journal of Technology*, *13*(7), 1393. https://doi.org/10.14716/ijtech.v13i7.6184

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.