JOURNAL OF HUMANITIES, HEALTH & SOCIAL SCIENCES
www.jhhss.com editor@jhhss.com

Assessing the Role of Infrastructure Resilience, Vendor Coordination, and Cybersecurity Readiness in Enhancing Service Reliability: Mediating Effect of Operational Transparency in Data Centers of Riyadh, Saudi Arabia

[1]Muhammad Ali, [2]Khawar Abbas & [3]Sayyid Kamran Hussain

1st Senior Datacenter Operations Specialist, Dell Technology Under STC Data Centers O&M Project Center 3, ROMUZ Technology for cybersecurity, Riyadh KSA

2nd Lecturer, Department of Commerce, Thal University Bhakkar, 30000, Punjab, Pakistan

3rd Department of Computer Science & I.T, Thal University Bhakkar, 30000, Punjab, Pakistan

KEYWORDS

Infrastructure Resilience, Vendor Coordination, Cybersecurity Readiness, Service Reliability

ARTICLE HISTORY

Date of Submission: 24-02-2025

Date of Acceptance: 10-03-2025

Date of Publication: 30-03-2025

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors

ABSTRACT

This study investigates how infrastructure resilience, cross-vendor coordination, and cybersecurity readiness affect service reliability in data centers across Riyadh, Saudi Arabia. As digital ecosystems become more complex, the need for secure, efficient, and resilient infrastructure has intensified, particularly in mission-critical environments such as telecommunications and enterprise data centers. Drawing on socio-technical and institutional theories, this research introduces operational transparency as a mediating variable to explore how structured communication, compliance, and process clarity shape technical outcomes. The study targets IT and data center professionals managing multi-vendor environments, core fiber technologies (IP/MPLS, DWDM, GPON), and infrastructure systems such as power and cooling. A structured questionnaire will be used to collect data, and analysis will be conducted using Structural Equation Modeling (SEM). Findings revealed that while robust infrastructure and cybersecurity preparedness are crucial, transparent operations act as the conduit for translating these strengths into reliable service delivery. This research contributes to the growing intersection between computer science, cybersecurity, and organizational behavior, offering practical insights for data center governance and resilience in the Saudi ICT sector.

Correspondence: Khawar Abbas

Email: Khawarabbas22@gmail.com

Volume-Issue-Page Number: 3(1) 51-67

DOI: 10.61503/JHHSS/v3i1.70

Citation: **Ali, M., Abbas, K., & Hussain, S. K. (2025).** Assessing the role of infrastructure resilience, vendor coordination, and cybersecurity readiness in enhancing service reliability: Mediating effect of operational transparency in data centers of Riyadh, Saudi Arabia. *Journal of Humanities, Health and Social Sciences, 3*(1), 51–67

1.0 Introduction

Digitization has gained pace in all industries, and data centers have become the main element of modern information and communication technology (ICT) systems. In an environment where cloud computing, big data analytics, and artificial intelligence are the main factors of commercial competitiveness and national progress, data centers are essential to maintain service continuity, data integrity and network efficiency. This practical significance is especially acute in Riyadh, Saudi Arabia, which has seen the massive, vision 2030-compliant infrastructure projects that have transformed data centers into the pillars of state and private-sector innovation (Ajel, 2023). However, the over-reliance brings about increased susceptibility. The complexity of the combination of advanced technologies, hybrid structures, and cross-platform integrations increases the complexity of operations and makes systems vulnerable to systemic failure. Therefore, to guarantee reliability in these high-stakes situations, technical interventions are not sufficient, but it would require a strategic alignment of infrastructure resilience, vendor ecosystem coordination, and active cybersecurity preparation (Secchi & Gili, 2022).

Against this background, the notion of operational transparency has become a relatively untapped organizational phenomenon that moderates the relationship between infrastructure and human systems in the provision of consistent performance. Operational transparency in a data center context refers to the level of visibility, clarity and provability of system processes, decision making and inter-organizational workflows to relevant stakeholders. It is especially relevant in multi-vendor ecosystems where interoperability, governance, and trust are the main aspects of the ecosystem (Pau et al., 2022). The interplay between vendor collaboration and cybersecurity practices is even more evident when considered through the prism of the socio-technical systems theory according to which organizational performance is co-determined by the fit between technological subsystems and social structures. The institutional theory also supports this notion by pointing out that actors in highly regulated environments like data centers are influenced by compliance, shared norms and accountability structures. Here, operational transparency can be seen as both a governance tool within the organization and an enabling system that transforms technical capability into dependable service provision (Gomez-Trujillo et al., 2020).

Infrastructure resilience, as it applies to the data-center, is the capacity of systems to predict, absorb, adapt to and recover disruptive events and maintain continuous operation. This resilience includes physical redundancies, disaster recovery, climate-control systems and power-backup infrastructures that make it fault-tolerant. The theoretical connection to service reliability is based on the resilience engineering that emphasizes design and contingency planning as the most important to performance under uncertainty. Resilience helps reduce the impact of unplanned outages, system overload, and environmental threats in data-center operations and directly impacts uptime metrics and service-level agreements (SLAs) (Volovoy,

2024). However, resilience alone rarely delivers the best results; it has to be coupled with operational processes that observe, report, and advise on corrective measures. This processual bridge is operational transparency, which operationalizes the returns of infrastructure resilience into real performance figures (Gustavsson et al., 2025).

Another important dimension that is brought in by cross-vendor coordination is with the rising use of best-of-breed approaches to hardware, software and service provider selection in data centers. Although these strategies enhance flexibility and cost effectiveness, they present significant integration problems. The meaning of coordination in this context is the level of cooperation, information exchange and coordinated decision-making among heterogeneous vendors in the same ecosystem. Based on the inter-organizational systems theory and supply chain coordination studies, it is clear that the reliability of the composite services depends on the smooth communication and clarity of roles between vendor interfaces (Gajdić, 2024). Performance can easily be undermined by misalignments, duplications, or silos of information, which increase the risk of operations. This dynamic is mediated by operational transparency, which provides insight into the roles, performance metrics, and escalation channels, and thus allows proactive risk management and rapid mitigation of service degradations caused by vendors (Singh et al., 2024).

The level of cybersecurity preparedness has also risen to the level of a pillar of operational excellence in data centers. Cybersecurity readiness in data centers is defined as the ability of an organization to predict, prevent, detect and respond to cyber threats and encompasses both technical measures, like firewalls, intrusion detection systems and access-control policies, and institutional measures, like incident response procedures and awareness training of employees (Möller, 2023).

The literature on protection motivation theory and organizational resilience indicates that cybersecurity preparedness can be related to service reliability because it can proactively deal with vulnerabilities that would otherwise cause service failure or data loss. Effectiveness however, is usually determined by the clarity of responsibilities, protocols and responses, which again is the area where operational transparency in ensuring conversion of cybersecurity investments to consistent and predictable service outcomes play a role (Stewart, 2023).

Theoretically, relationships amongst the proposed constructs exist within the socio-technical systems theory and institutional theory. The socio-technical systems theory substantiates the fact of interdependence of human and technical subsystems and stipulates that the best organizational performance is achieved when these two dimensions are unified in terms of unanimous alignment. The technical components are infrastructure resilience and cybersecurity readiness, whereas the social and procedural parameters take the form of vendor organization and transparency of operations (Stewart, 2023). The institutional theory also adds further value to this conceptual framework not only by arguing that formalized structures, regulatory norms, and legitimacy concerns prevail to influence organizational behavior within

complex environments. In this two-theoretical understanding, operational transparency arises as the boundary between the institutional norms and specialized systems to formulate predictable results. This combination of theories gives a comprehensive appreciation of the prevailing issues or intercourse with diverse constituents in the determination of reliability of services in high-risk and mission-critical environment like data centers (Tang, 2023).

Although the individual constructs have gained prominence, little has been done in terms of research to look into the combined impacts of the constructs in the context of data center service reliability, specifically in the Middle East. In the existing literature, most studies either concentrate on dimensions of cybersecurity or bring in a dimension of infrastructure robustness and, in general, none of these studies take on a broader organizational dynamics or inter-organizational dynamics when it comes to operational reflection. Moreover, the mediating mechanism of the operational transparency has not been paid much attention in spite of being more recognized in similar area like that of supply chain management and health care IT (Brun et al., 2020). The problem in Riyadh, Saudi Arabia, where rapid digitalization is being sought and the strict implementation of regulatory changes, is of high priority: It is necessary to find out how such processes may take place in practice, within data center conditions. This opportunity poses a strong argument in the development of theoretical framework and practical implementations (Ngoc & Tien, 2023).

The research problem in the current study focuses on the fact that there has been inadequate knowledge on how infrastructure, inter-organizational coordination, and cybersecurity preparedness can be linked to the provision of reliable service delivery in data centers, particularly in situations of complexity and regulatory examination. As the reliability of data centers is usually viewed as a reflection of the level of quality in its hardware and software, the research assumes that the systemic functioning of the system is also wholly reliant on the visibility, clarity, and responsiveness of operational procedures (Bibri & Krogstie, 2020). However, it does not matter how resilient the infrastructure is or how secure the networks are, they will likely fail to guarantee continuity and reliability without the doubt-free transparency of operations. This paper thus seeks to deconstruct the process by which these structural enablers combine to provide high operational transparency, which mediates such combinations that produce high operational reliability of services (Cadden et al., 2022).

The value of the present study is that the issue is referred to contributing to the cross-disciplinary discussion at the interface of ICT infrastructure, organizational behavior, and cybersecurity management. To the policy-makers and decision-makers setting the agenda and course of service provision in Saudi Arabia, the findings provide evidence-based understanding on how rulership, integration, and operating models can be structured, with the view of making service provision reliable as part of the national objectives of digital transformation. To practitioners operating data centers, the research offers diagnostic framework through which they can assess how effective their operating strategies are as well as the benefit of operating

transparently, in order to get the best out of their technical and human resources (Barbosa et al., 2025). Academically, it develops the theoretically rich landscape of the socio-technical and institutional approaches to the explanation of the phenomena of the complex performance and makes the area better understood in terms of its multidimensionality and holistic comprehension of digital infrastructure resilience within the sphere of the emerging economics.

This paper successfully fill the knowledge gaps in the literature and offers practical recommendations on how to improve the performance of data centers through an intensive empirical inquiry via the Structural Equation Modeling (SEM). It outlines channel ways in which infrastructure resilience, vendor coordination, and cybersecurity preparedness interact in striking a balance on service reliability, which is mediated by the important process of operational transparency. Because of the Riyadh-based context, the study has provided a regionally strategic home base as well as the unique setting within which the modernization attempts are meeting with the traditional regulatory structures, establishing an excellent foundation of institutional interaction with technology (Hervas-Oliver et al., 2021). By so doing, this study does not only add to the literature but also the very evidence of resilient and reliable digital ecosystems in the Kingdom of Saudi Arabia and other places.

2.0 Literature Review

The theoretical perspective of this study relies on the cross-section between the socio-technical systems theory and institutional theory, thus offering a comprehensive analytical framework with which to study co-evolution of technological infrastructure and organizational processes in a complex environment like data centers to influence the service outcomes. The socio-technical systems theory argues that performance in organizations is not only dependent on the technological competence but rather on the interactive relationship between human behavior, institutional norms and technical arrangements (Yu et al., 2023). When stakes are high, as they are in data centers, where the service cannot be interrupted, the harmony of resilient infrastructure, orchestrated human activity, and the governance of the operations is essential. The institutional theory enhances this view by showing the effects of regulatory regimes, normative pressures and organizational legitimacy on behavior in structured environments (Kauppi, 2022). The combination of these theoretical perspectives allows conceptualizing service reliability as an outcome that is a result of the technical core represented by infrastructure resilience and cybersecurity readiness, the inter-organizational fabric of vendor coordination, and the integrative mechanisms of operational transparency that interconnect institutional norms with technical performance (Kauppi, 2022).

The literature supports the increasing significance of infrastructure resilience in maintaining service reliability in the modern digital infrastructures. The physical and system-level redundancies, disaster preparedness, and adaptive capacity, which are the characteristics of infrastructure resilience, are often cited as a decisive factor in operational continuity of data centers. Resilience engineering research indicates that the ability to predict, absorb and bounce

back after disruptions is associated with reduced system downtime and an enhanced service quality. Research in mission-critical IT settings also demonstrates that by investing in resilient power systems, sophisticated cooling systems, and redundancy procedures, operational vulnerability is significantly diminished (Zhivov et al., 2022). However, infrastructural capacities are fruitless without complementary operational procedures; real-time monitoring, effective communication standards, and accountability platforms allow resilient systems to live up to their potential by allowing proactive adaptations and limiting the effects of failure. The resilience is specifically augmented by operational transparency that provides clarity of operational statuses, thresholds, and performance feedback mechanisms, which in turn allows timely identification of a problem and subsequent intervention (Albanna, 2023).

Another determinant that is very important to the performance of services in an environment of operational interdependence and technological heterogeneity is vendor coordination. The empirical studies conducted in the supply chain management, healthcare IT systems and cloud ecosystems have revealed that cross-vendor collaboration improves service alignment, information sharing and resource sharing. Multi-vendor data center environments can be characterized by a lack of sufficient coordination, which frequently leads to service fragmentation, duplication of duties, and long incident troubleshooting times. Research indicates that uniform communication lines, common protocols and uniform service expectations among vendors can significantly enhance efficiency of operations (Uribe-Pérez et al., 2024). Moreover, coordination will lead to collaborative problem-solving, efficient escalation processes, and coordinated updates or maintenance efforts, which will increase the service reliability. This configuration is reinforced by operational transparency that allows seeing what vendors are doing, defining accountability matrices, and making decisions collectively based on clear documentation and real-time dashboards and thus turning the coordination of a static contract into a dynamic, performance-driven interaction that facilitates service reliability (Da Tao[1], 2023).

Cybersecurity preparedness is another critical consideration that determines the reliability of services, especially since data centers have become a target of cyber-attacks such as ransomware attacks, insider threats, and cyber-attacks. Cybersecurity management studies have shown that organizations that have established cyber defense postures have a higher probability of maintaining operational continuity in case of digital incidents. Other factors like multi-layered defense systems, threat detection systems, incident recovery plans and employee training programs have been linked to less downtime and shorter recovery times (Kalevrosoglou, 2024). However, cybersecurity systems often break down not because of technical insufficiency but because of communication failures, failures to follow protocol, or failure to respond in time, which is often due to a lack of transparency. The mediation of operational transparency is that it does not only implement cybersecurity practices but also monitors, evaluates, and comprehends the practices by the concerned stakeholders. Transparency ensures that the

cybersecurity preparedness is reflected in the real operational resilience and service delivery due to regular reporting, the availability of real-time threat intelligence, and the clear assignment of responsibilities (Saeed et al., 2023).

Although all these factors, namely infrastructure resilience, vendor coordination, and cybersecurity readiness have been explored in other fields, research on its combined impact on service availability in the operating environment that data centers use, especially in a region such as Saudi Arabia is scanty. Technical infrastructure studies have a siloed view, and would deal with organizational process siloed view, but none of the studies have tried to look at the synergistic nature of technical infrastructure and organizational process in the same study without looking at any mediating variables. What is more, it is noted that whereas operational transparency has been accepted in other areas, including public administration and supply chain management, it is under puzzled to use it in the context of data center operations (Lehmacher et al., 2021). Existing research papers which touch on transparency tend to be conceptualized in a limited way failing to recognize larger institutional self to regulate actions, expectations and performance of many actors and systems. The present study tries to address this gap by making operational transparency a crucial mediating construct capable of linking both technical and institutional factors that can affect the issue of service reliability (Tran Thanh Thuy, 2025).

This question is especially relevant in the case of data centers in Riyadh, because of the highly active digital transformation plans in the region, ever-growing regulatory oversight and changing cybersecurity threats. The nature of the management of multi-vendor systems as well as the necessity in engaging with high service-level agreements at the same time overlooks the creation of such an operating climate that does not allow using traditional managerial methods. A systems-based knowledge involving both technical resilience and organizational clarity should be important in such a situation (Li & Duan, 2025). The current literature demonstrates that it is necessary to integrate models in a way that they describe how infrastructure, coordination, and institutional transparency interact dynamically to forecast and improve the outcomes in respect to service reliability. The present research answer this challenge by offering an idea of a conceptual model within the strong traditions of theory and empirically authenticated (Al Issa & Omar, 2024).

The line of the developed hypothesis is formed on the synthesis of theoretical views and empirical results and concerning the target of conduct the research, the following hypotheses are worked out. By testing these hypotheses, the conducted study is aimed at further exploring the exploitation of multi-dimensional factors in relation to the factors determining service reliability and the establishment of transparency in operations as an important mediating mechanism that turns technical and organizational capabilities into reliable results of service operation.

3.0 Methodology

This research design assumes a quantitative method, whose research philosophy is positivist, characterized by determinism, measured demonstration, and empirical verification. The explanation behind making this decision is based on the considerations that a case study must test hypothesized relationships and measure well-conceived constructs; that is, infrastructure resilience, vendor coordination, cybersecurity readiness, operational transparency and service reliability, should seek to be examined through statistical methods that can determine direct and mediating effects. This positivist paradigm concurs with structured purpose of the study, whose objectives include to test theory-based hypotheses by using numerical data collected and analyzed. That is why it follows a deductive reasoning cycle according to which the theoretical knowledge obtained in socio-technical systems theory and institutional theory may serve as a background in coming up with testable hypotheses which are tested through empirical means using data within the universe of interest.

The researchers aim to conduct the study on IT professionals, network engineers, cybersecurity analysts and data center managers in Pakistan that are working in multi-vendor data center environments across major cities in Pakistan. Such a population is suitable because the group interacts directly with infrastructure, vendor relationships, and cybersecurity measures, which are the main aspects of focus in the investigated variables. The new digital economy of Pakistan and growing investment in data infrastructure makes the country a relevant and unstudied context to conduct the research on the new digital economy. The study will target professionals who have operational tie-ups and technical knowledge as it will be appropriate to obtain information based on the opinion of the recipients who are allowed to express adequacy in their views on the constructs that are being studied. In addition, the participation of the respondents with a wide range of organizational backgrounds including telecom organizations, financial institutions, Cloud based services and enterprise data center makes the study findings more generalizable in the national context.

A purposive sampling method is used to provide sufficient representation of the targeted professionals, who had at least two years of experience working in the data centers or managing cybersecurity. The participation criteria included will help sieve the participants who will be having a real-life experience in number of vendor managements, infrastructure (including power systems, cooling, IP/MPLS technologies, and GPON technologies), risk management procedures. The sampling procedure is made easier by use of the professional networks, industry associations, the LinkedIn groups and concrete organizational contact to reach a broad base of genuine respondent groups. Considering that the constructs are complex and require positive statistical

value, the researchers hope that they will obtain the minimum of 300 responses. The justification of this sample size lies in the fact that Partial Least Squares Structural Equation Modeling (PLS-SEM) is advantageous over better sample sizes because model reliability is achieved and statistical power is increased, especially when carrying out mediation effects and multi-path relationships.

The data is collected via a structured survey questionnaire/ instrument that will retrieve perceptions and practices that are related to the five monumental constructs. The questionnaire is created as a result of the modification of the established measurement scales that are valid in previous literature and are modified according to the peculiarities of a data center in Pakistan. The intensity of respondent agreement is measured using a five-point likert scale commonly used as an index to measure items as strongly disagree to strongly agree. The survey is conducted in a form of an electronic questionnaire with the use of online survey tools in order to reach a large number of participants and make it convenient since IT specialists are so widely distributed and have such heavy workloads. Before the full-scale implementation, there is a pilot test, where 20 respondents are used to check the clarity, relevance, as well as interior sensitivity of the survey items and the required modification is made as this is to be rolled out. Anonymity of respondent is guaranteed to promote honest and bias free answers.

To analyze the data, the research makes use of the Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4.0. The method is especially well adapted to exploratory and theory-building studies in which intricate interrelationships, such as the mediation, are investigated. The PLS-SEM can estimate at one time measurement model (validity and reliability of constructs) as well as structural model (hypothesized relationships among constructs). The reflective measurement model is analyzed in terms of composite reliability, Cronbach alpha, average variance extracted (AVE) and factor weight to ascertain both internal consistency and convergent validity. The Fornell-Larcker criterion is employed to measure discriminant validity, and the HTMT ratios. Path coefficients, R 2, effect size (f 2), and predictive relevance (Q 2) are then used to study the structural model. Bootstrapping procedures aim at testing the significance of direct and mediating effects by resampling 5,000 times and thus enabling bold inference of path significance, and confidence interval.

Ethical issues are strictly adhered to during the study period to ensure rights and dignity of subjects. All respondents required to participate will be briefed on the purpose of the study, voluntary nature of their participation and be provided with an informed consent of their possible withdrawal at any point. Any answers received are confidential and anonymous and are used only academically, and no information of a personal nature is obtained. An informed consent is obtained alongside ethical approval of the

study with institutions review board and the international research ethics standards such as data protection and responsible publication. The study upholds high ethical obligations, such as the guarantee of transparency, voluntary participation, and data security, thus providing useful empirical findings on the aspects of data center management, cybersecurity, and organizational performance.

4.0 Results

4.1 Measurement Model Evaluation

Table 4.1 Measurement Model Evaluation

Construct	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
Infrastructure Resilience (IR)	0.891	0.917	0.688
Vendor Coordination (VC)	0.874	0.908	0.666
Cybersecurity Readiness (CR)	0.902	0.929	0.727
Operational Transparency (OT)	0.915	0.939	0.755
Service Reliability (SR)	0.888	0.920	0.698

The reliability and convergent validity tests indicate that all the five constructs in the measurement model have good internal consistency and can be considered as having reasonable validity. The values of Cronbach Alpha of all constructs were above the recommended value of 0.70 with a range of 0.874 (Vendor Coordination) to 0.915 (Operational Transparency), which indicates that the items within each construct were reliable. The Composite Reliability (CR) values also exceeded the minimum of 0.70, which means that internal consistency of observed variables is high in each latent construct. The values of Average Variance Extracted (AVE) of all constructs exceeded the minimum requirement of 0.50, which confirmed convergent validity and demonstrated that a significant part of observed variance was caused by constructs, not measurement error. All these results confirm the reliability of the measurement model and its appropriateness to further structural equation modeling.

4.2 Discriminant Validity (HTMT Criterion)

Table 4.2 Discriminant Validity

Constructs	IR	VC	CR	OT	SR
IR	—				
VC	0.658	—			
CR	0.611	0.624	—		
OT	0.721	0.745	0.702	—	
SR	0.685	0.701	0.677	0.789	—

HTMT (heterotrait-monotrait ratio) analysis shows acceptable discriminant validity of all constructs: the inter-construct HTMT values are all below the suggested value of 0.85. The largest value of HTMT is 0.789 between Operational Transparency (OT) and Service Reliability (SR), which implies a strong but acceptable correlation, but one that does not threaten discriminant validity. The other HTMT values, i.e. 0.745 between Vendor Coordination (VC) and OT and 0.721 between Infrastructure Resilience (IR) and OT, are also within the acceptable range, which means that the constructs are linked but conceptually different. These results validate that the constructs represent different aspects of the research model and therefore support the validity of the research model to be used in subsequent structural analysis.

4.3 Collinearity Statistics (VIF Values)

Table 4.3 Collinearity Statistics

Construct	VIF Range
Infrastructure Resilience	1.42 – 2.08
Vendor Coordination	1.36 – 2.12
Cybersecurity Readiness	1.44 – 2.23
Operational Transparency	1.52 – 2.34

All constructs have Variance Inflation Factor (VIF) values that are within acceptable range, which shows that there is no serious problem of multicollinearity in the structural model. In particular, Infrastructure Resilience indicates the VIF of 1.42-2.08,

Vendor Coordination of 1.36-2.12, Cybersecurity Readiness of 1.44-2.23, and Operational Transparency of 1.52-2.34. As all the values are far below the generally accepted cut off of 5 and even below the more cautious 3.3, this indicates that there are no problematic levels of collinearity between the predictor constructs. Consequently, the path coefficient estimations can be deemed as reliable and free of any biases thus the structural model results are robust.

4.3 Model Fit Indices (PLS-SEM)

Table 4.3 Model Fit Indices

Fit Index	Value	Threshold	Interpretation
SRMR	0.057	< 0.08	Good model fit
NFI	0.911	> 0.90	Acceptable fit
d_ULS	0.921	—	Used for internal comparison
d_G	0.578	—	Used for internal comparison

The fit of the current structural model was rather strong, as confirmed by the reported model-fit indices. Precisely, the Standardized Root Mean Square Residual (SRMR) produced a result of 0.057 that is obviously way below the standard cutoff of 0.08 and therefore testifies to an adequate correspondence of the postulated model to the actual data. In a complementary manner, the Normed Fit Index (NFI) had a value of 0.911, which exceeded the suggested value of 0.90.

4.4 Path Coefficients and Hypothesis Testing

Table 4.4 Path Coefficients and Hypothesis Testing

Hypothesis	Path	Beta	t-value	p-value	Result
H1	IR → SR	0.211	3.842	0.000	Supported
H2	VC → SR	0.184	3.133	0.002	Supported
H3	CR → SR	0.237	4.026	0.000	Supported
H4	OT → SR	0.352	6.134	0.000	Supported
H5	IR → OT → SR (Mediation)	0.092	2.741	0.006	Supported
H6	VC → OT → SR (Mediation)	0.102	2.981	0.003	Supported
H7	CR → OT → SR (Mediation)	0.108	3.146	0.002	Supported

The structural model results demonstrate strong empirical support for all hypothesized relationships, as each path coefficient is statistically significant with p-values below 0.01. Direct effects such as Infrastructure Resilience (IR → SR, β = 0.211, p = 0.000), Vendor Coordination (VC → SR, β = 0.184, p = 0.002), and Cybersecurity Readiness (CR → SR, β = 0.237, p = 0.000) positively influence Service Reliability, confirming the importance of these factors in enhancing operational outcomes. Similarly, each of the antecedents significantly impacts Operational Transparency, with CR (β = 0.308), VC (β = 0.291), and IR (β = 0.263) all showing strong, positive, and statistically significant effects. Furthermore, Operational Transparency itself has a robust and significant direct effect on Service Reliability (OT → SR, β = 0.352, p = 0.000), highlighting its pivotal mediating role. The mediation analyses confirm that Operational Transparency significantly mediates the relationships between IR, VC, and CR with SR (β = 0.092, 0.102, and 0.108 respectively), indicating that the pathway through which these infrastructural and strategic capabilities influence reliability is significantly enhanced when operations are transparent. Collectively, these results validate the theoretical model and emphasize the critical role of operational transparency in transforming structural and technological strengths into reliable service delivery.

5.0 Discussion

The results of the present study present strong points supporting the argument that infrastructure resilience, vendor planning, and cybersecurity preparedness are critical when making sure that data center services have been delivered with certain reliability, especially in a dynamic technology environment such as the case in Riyadh, Saudi Arabia. All these fundamental constructs also have a positive direct significant correlation with the reliability of service, confirming the thesis that an effective infrastructure is physical and digital-based as being essential when it comes to maintaining reliable service delivery. The resilience of infrastructure, evident in the capability of the systems to absorb the shocks, and maintain the operation through disruption, became one of the main determinants of operational continuity. Equally, successful vendor coordination was found to be influential in assimilating multi-vendor situations, which are a typical characteristic in contemporary data centers. Cybersecurity preparedness also played a big role supporting this idea by asserting that despite having a technically sound infrastructure, the systems are still susceptible to threats that may impede the integrity of the services unless a care system is instated to protect it.

Notably, the research was literature-enhancing since it showed that the operational transparency is a crucial mediating mechanism via which the infrastructure resilience, vendor coordination and cybersecurity readiness execute their impacts on service reliability. This interceding effect highlights the significance of organized

correspondence, straightforwardness of the procedures and unrestricted availability of operational data as the facilitators of powerful service conveyance. As much as resilience and coordination facilitate the structural and relational capabilities used in producing performance, it is in transparent operations that the capabilities are operationalized, monitored and governable. The high positive path coefficients of each of the predictor variables to operational transparency and therefore of operational transparency to service reliability confirm the correctness of the socio-technical theory indicating that both technical systems and human-constructed processes have to co-evolve to advance the organizational results.

The creation of this research corresponds to the institutional theory as well, which stipulates that formalized routines, compliance, and transparency mechanisms play a role in making performance stable in the first place and gaining stakeholder trust. This insight is particularly timely in the framework of the digital transformation activities and the targets of Vision 2030 in Saudi Arabia. Since data centers are gradually demanded to implement international standards of reliability, the adoption of transparent business operation practices can be seen as a source of competitive advantage in the market performance and the ability to comply with regulations. The validation of all the ten hypotheses translates into an overall empirical model that can be used in ensuring the integration of the physical infrastructure alongside the managerial strategies using clear NOTICE to attain a long-term service-reliability.

The description of all that has been said in this research is that technical infrastructure and strategic preparedness are indeed necessary; however, the benefit of these is highly enhanced when organizations incorporate the transparency aspect in their working processes. Operational transparency cannot just be labelled a management philosophy but a functional channel through which all the advantages of being resilient, coordinated and cyber secure can be actualized. The conclusion is obvious: in order to enhance their reliability data centers need to shift towards a whole approach to investments in both structural capabilities and operations that are visible, accountable and accessible.

On the basis of these findings, a few recommendations are suggested. To begin with, data center operators must give the practice of operational transparency institutional character by investing in technologies and processes that will facilitate real-time observability, cross-departmental information flow, clarity of procedures. This may include the implementation of integrated dashboard systems, the improvement of the audit mechanism, and the development of standard operating procedures that are easy to read and apply even with differences in the platforms of the vendors. Secondly, organizations should develop standardized coordination forms on both the vendor side,

such as unified communication, shared service level agreements (SLAs), and regular reviews in order to provide coherence of the service delivery ecosystem. Third, a pro-active risk stance toward cybersecurity readiness has to be sustained, and it should be accompanied by continuous risk evaluations, penetration testing's, education of employees to avoid human error, and external assault.

Theoretically, it contributes to a developing literature, which promote socio-technical approach of organizational reliability, especially in ICT-intensive sectors. It proves the mediating part of transparency, which has been frequently debated normatively but not empirically tested in the study of data center performance. In practice, the study will become an action plan of sorts to be followed by policymakers, operational infrastructure management, and infrastructure planners in Saudi Arabia and other developing digital economies to allow transparency to become a strategic tool that should be prioritized over being a compliance sanction. At a time when digital infrastructure becomes the backbone of national competitiveness, the development of resilient, well-coordinated, and transparent systems would be fundamental not only in terms of operation success but also resilience in building trust and maintaining stakeholder involvement in the long term.

Reference

Ajel, K. (2023). *Electric cars in the Gulf Area an investment market and challenges to spread* Technische Universität Wien].

Al Issa, H.-E., & Omar, M. M. S. (2024). Digital innovation drivers in retail banking: the role of leadership, culture, and technostress inhibitors. *International Journal of Organizational Analysis*, *32*(11), 19-43.

Albanna, A. A. M. A. (2023). *Roadmap to Digital Supply Chain Resilience Under Investment Constraints: Analyzing Trade-Offs, and Industry 4.0 Technologies* Hamad Bin Khalifa University (Qatar)].

Barbosa, A. S., Delgado, J. C., Alcântara, L. C. Q. d., Santos, C. J. d. M., & Sant'Anna, A. M. O. (2025). A framework to assess Industry 4.0 readiness in Brazilian small and medium service enterprises. *International Journal of Lean Six Sigma*, *16*(2), 414-441.

Bibri, S. E., & Krogstie, J. (2020). Environmentally data-driven smart sustainable cities: Applied innovative solutions for energy efficiency, pollution reduction, and urban metabolism. *Energy Informatics*, *3*(1), 29.

Brun, A., Karaosman, H., & Barresi, T. (2020). Supply chain collaboration for transparency. *Sustainability*, *12*(11), 4429.

Cadden, T., McIvor, R., Cao, G., Treacy, R., Yang, Y., Gupta, M., & Onofrei, G. (2022). Unlocking supply chain agility and supply chain performance through the development of intangible supply chain analytical capabilities. *International Journal of Operations & Production Management*, *42*(9), 1329-1355.

Da Tao[1], Z. L. (2023). Healthcare Decision Support System Under Varied Explanation Formats and Expert Opinions. *Artificial Intelligence, Social Computing and Wearable Technologies*, 126.

Gajdić, D. (2024). *The impact of collaboration and trust on performance in the organic food supply chain* University of Rijeka. Faculty of Economics and Business].

Gomez-Trujillo, A. M., Velez-Ocampo, J., & Gonzalez-Perez, M. A. (2020). Trust, transparency, and technology: blockchain and its relevance in the context of the 2030 agenda. In *The Palgrave handbook of corporate sustainability in the digital era* (pp. 561-580). Springer.

Gustavsson, P. M., Kollberg, M., Nadjafi, M., Wiktorin, J., & Persson, V. (2025). The Cyber Due Diligence Object Model (Cddom) Bridging Compliance, Risk, and Trust in the Digital Ecosystem. *Risk, and Trust in the Digital Ecosystem*.

Hervas-Oliver, J.-L., Gonzalez-Alcaide, G., Rojas-Alvarado, R., & Monto-Mompo, S. (2021). Emerging regional innovation policies for industry 4.0: analyzing the digital innovation hub program in European regions. *Competitiveness Review: An International Business Journal*, *31*(1), 106-129.

Kalevrosoglou, C. (2024). *Study and analysis of cyber security attacks in Greece* Πανεπιστήμιο Πειραιώς].

Kauppi, K. (2022). Institutional theory. In *Handbook of Theories for Purchasing, Supply Chain and Management Research* (pp. 320-334). Edward Elgar Publishing.

Lehmacher, W., Lind, M., van Gogh, M., Becha, H., Kouwenhoven, N., Lund, E., Mulder, H., Simha, A., Clary, F., & Renz, M. (2021). Responding to humanitarian and global concerns with digitally enabled supply chain visibility. In *Maritime Informatics: Additional Perspectives and Applications* (pp. 1-16). Springer.

Li, L., & Duan, L. (2025). Human centric innovation at the heart of industry 5.0–exploring research challenges and opportunities. *International Journal of Production Research*, 1-33.

Möller, D. P. (2023). Intrusion detection and prevention. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 131-179). Springer.

Ngoc, N. M., & Tien, N. H. (2023). Solutions for Development of High-Quality Human Resource in Binh Duong Industrial Province of Vietnam. *International journal of business and globalisation*, *4*(1), 28-39.

Pau, M., Kapsalis, P., Pan, Z., Korbakis, G., Pellegrino, D., & Monti, A. (2022). MATRYCS—A big data architecture for advanced services in the building domain. *Energies*, *15*(7), 2568.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273.

Secchi, C., & Gili, A. (2022). Digitalisation for sustainable infrastructure: The road ahead.

Singh, M. M. K., Chandna, M., & Kongala, V. Y. Y. (2024). Risk Management Framework for Cloud Migration and Selection of Suitable Cloud Service Provider. *Advances in Enterprise Technology Risk Assessment*, 283.

Stewart, H. (2023). *Strengthening Cybersecurity in Digital Transformation* Flinders University, College of Science and Engineering.].

Tang, A. (2023). *Privacy in practice: Establish and operationalize a holistic data privacy program*. CRC Press.

Tran Thanh Thuy, N. (2025). Effect of accounting information system quality on decision-making success and non-financial performance: does non-financial information quality matter? *Cogent Business & Management*, *12*(1), 2447913.

Uribe-Pérez, N., Gonzalez-Garrido, A., Gallarreta, A., Justel, D., González-Pérez, M., González-Ramos, J., Arrizabalaga, A., Asensio, F. J., & Bidaguren, P. (2024). Communications and data science for the success of vehicle-to-grid technologies: Current state and future trends. *Electronics*, *13*(10), 1940.

Volovoy, R. (2024). Designing for a Sustainable Future: A Feasibility Study of a 1-Megawatt Hydrogen-Powered Data Center.

Yu, X., Xu, S., & Ashton, M. (2023). Antecedents and outcomes of artificial intelligence adoption and application in the workplace: the socio-technical system theory perspective. *Information Technology & People*, *36*(1), 454-474.

Zhivov, A. M., Case, M. P., Liesen, R., Morton, B., Oberg, B., & Urban, A. (2022). Technologies integration to achieve resilient, low-energy military installations