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

Managerial Role of Network Infrastructure, Cybersecurity Tools, and Systems Monitoring in Enhancing IT Service Reliability: A Case Study of GBM Abu Dhabi, UAE

[1]Muhammad Umar Ilyas, [2]Tauseeq Iqbal & [3]Thair Matila

1st Senior Network Support Engineer, GBM, Abu Dhabi.

2nd Research Scholar, GCU Faisalabad Sahiwal campus.

3rd Admin officer, Bahauddin Zakariya university Multan

KEYWORDS

Network Infrastructure, Cybersecurity Tools, Systems Monitoring, IT Service Reliability

ARTICLE HISTORY

Date of Submission:18-10-2024
Date of Acceptance:15-11-2024
Date of Publication:31-12-2024

Funding

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

ABSTRACT

This study examines the managerial impact of network infrastructure robustness, cybersecurity tool integration, and proactive systems monitoring on the overall reliability and performance of IT services within enterprise environments. The objective is to analyze how the structured deployment of advanced routing and switching technologies, security systems, and monitoring platforms contributes to IT service continuity and operational excellence at GBM – Abu Dhabi, a leading technology provider in the UAE. Using a mixed-method approach, data were collected from 35 network engineers, IT managers, and system administrators through surveys and interviews. The findings indicate that strategic management of firewalls, VPN solutions, and access control mechanisms (e.g., Cisco ISE, Forti-Authenticator) significantly reduces vulnerability exposure and strengthens endpoint defense. Efficient use of monitoring tools such as PRTG, Riverbed, and Cisco Prime enhances visibility, allowing faster incident detection and resolution. Furthermore, the integration of high-availability protocols, load balancing, and wireless scalability contributes to improved service delivery. The study emphasizes that managerial oversight, continuous documentation (e.g., ISO Smart Inventory), and cross-vendor skill development are crucial for sustaining performance in complex IT ecosystems.

Correspondence: Tauseeq Iqbal

Email: maliktauseeq66@gmail.com

Volume-Issue-Page Number: 2(4) 89-103

Citation: Ilyas, M. U., Iqbal, T., & Matila, T. (2024). Managerial role of network infrastructure, cybersecurity tools, and systems monitoring in enhancing IT service reliability: A case study of GBM Abu Dhabi, UAE. Journal of Humanities, Health and Social Sciences, 2(4), 89–103

1.0 Introduction

The ability to deliver and rely on IT services today is crucial for any business looking to succeed and compete effectively. Because business processes, how companies interact with customers and data are now digital, IT now has a major role in driving growth and innovation. Because of this approach, organizations have to put in place advanced network systems, strong cybersecurity tools and tight systems monitoring to keep their IT services running successfully and safely (Mishra, 2022). The UAE and Abu Dhabi in particular stand out as examples of digital transformation, thanks to the way technology, government and management work together to promote IT excellence. GBM Abu Dhabi demonstrates this change by spending a lot on advanced technology and management approaches to keep their IT services trustworthy and uninterrupted. Because technology is now used more widely, IT infrastructures are more vulnerable to system failures and security risks, so the way managers handle technology becomes vitally important (Djenna et al., 2021).

The base of IT service reliability is a robust network infrastructure that includes all the hardware, software, communication protocols and setup needed for information to be sent between devices. A weak network backbone makes organizations vulnerable to more downtime, loss of important data, poor service quality and eventual operational inefficiency and upset customers (Anderson et al., 2021). This means that cyber threats, including malware, ransomware and intrusions backed by governments, are driving the need for powerful tools that can detect, prevent and manage such risks. These tools are firewalls, intrusion detection systems, encryption techniques and endpoint protection solutions that act as important barriers in IT systems (Hadi et al., 2024). In addition, ongoing monitoring of systems uses live surveillance and diagnostic techniques to spot issues, slowdowns and problems before anything goes wrong. By monitoring systems, organizations can switch from reacting to problems to managing them ahead of time, resulting in much better IT services for users.

Although research has mainly covered the technology elements of network infrastructure, cybersecurity and systems monitoring, the management approach needed for using and setting these technologies efficiently is still less understood, especially in the UAE. Having a manager in charge ensures IT assets are used to support important business goals, that resources are distributed effectively, a culture of safety is promoted and governance helps keep both risk and innovation under control (Al Astal et al., 2024). According to the RBV, firms can win in the competition by using special, valuable and difficult-to-reproduce resources such as their technical skills and managerial leadership. Similarly, the TOE framework shows that what happens inside an organization and in its surrounding environment can affect the success of technology adoption. When looking at IT service reliability, it becomes clear that using network infrastructure, cybersecurity and system monitoring successfully comes from

technology and the right actions taken by managers to use resources in the best way and address emerging obstacles (Safitra et al., 2023).

In spite of the fact that these elements are important, research still misses out on how a manager's role helps determine how reliable the IT service remains given strong network infrastructure, cybersecurity and regular monitoring. In most existing literature, different aspects are often studied separately or simply from a technical standpoint, while missing the need for managers to coordinate them effectively (Villena-Manzanares et al., 2020). Also, little research has examined these connections in the UAE which is a rapidly digitalizing country with new cyber laws, changing cultural values and a range of organizational growth among companies. By reviewing GBM Abu Dhabi, we can examine these dynamics because the organization must deal with technological challenges, threats from different sources and challenges in managing operations (Ghadi et al., 2024). Therefore, the main research problem focuses on exploring how managers influence the use and effectiveness of network equipment, cybersecurity solutions and monitoring to support high-quality IT services. Solving this problem is necessary for organizations to keep running smoothly, comply with important rules on data and stay ahead of competitors in a fast-changing technology area (Espindola & Wright, 2021).

This study is valuable due to its contributions to both understanding and application. It broadens the IT service management conversation by combining RBV and TOE principles to explain how organizational leaders can maximize the use of technology for steady service performance. By adopting this view, we highlight that a strong management team helps organizations manage technology investments in ways that fit their situation and meet current demands. In practice, the results help IT executives, managers and policymakers in the UAE and comparable emerging digital economies find solutions. For professionals at GBM Abu Dhabi and similar organizations, this study points out the important strengths and management methods needed to get maximum use from technology and control risks. Based on these observations, policy and regulation can support both learning new technologies and developing managers, making sure the nation's digital infrastructure is strong. As a result, it is shown that reliable and sustainable IT services depend on both advanced tools and strong management in the modern and hazardous digital world.

It is necessary to explain that network infrastructure is built from a variety of parts—including routers, switches, servers, cloud services and channels—all working together to allow data to move within and outside an organization. Whether an IT system can withstand problems and keep up its services is decided by how these components are designed, how scalable they are, their redundancy and how secure they are (Zhang et al., 2022). The performance of a company's infrastructure is greatly affected by the way managers choose its network architecture, set capacity levels, pick its vendors and manage maintenance tasks.

Besides, the fast appearance of SDN and NFV technologies has introduced both new problems and opportunities for network management, so managers must use adaptive techniques to address flexibility and control potential issues (Rahman et al., 2025). As GBM Abu Dhabi serves clients who want their services available around the clock and who comply with international rules such matters are crucial.

Just like networks, cybersecurity tools are developing and are now essential for defending the IT systems of a company from both inside and outside dangers. There are various tools, including those around the perimeter, at endpoints, for access management, for data encryption and for security information and event management (SIEM). Because cybersecurity tools need to be in place, managers should always watch for new threats, prioritize security issues and make sure security policies support the overall business strategy (Kaplan et al., 2015). As cyber threats become harder to detect and respond to, managers must handle security tasks and imagine future risks, while still ensuring that operations go smoothly. Cybersecurity tools rely on a company's culture and efforts from managers to educate staff and encourage the reporting of incidents strengthen the organization's cybersecurity.

Systems monitoring covers the task of collecting and checking data from IT systems to pick up on any anomalies that could mean a fault is developing or a security incident is taking place. Monitoring systems that work well depend on real-time reports, alerts and predictions from artificial intelligence and machine learning to secure resources and avert failures. A manager is responsible for choosing the right monitoring devices, deciding what counts as acceptable performance, coordinating people to respond to issues and including monitoring results in making decisions about the company's strategy (Robert et al., 2022). Taking this approach helps prevent downtime, improves how the system is used and supports efforts to make things better all the time. GBM Abu Dhabi depends on advanced monitoring technologies to achieve SLAs and maintain customer satisfaction among competitors.

The connection between the three technological areas—network, security and monitoring—with IT service reliability is strong. A firm network foundation is needed for cybersecurity tools and monitoring systems to run well; however, any problems with cybersecurity or the network can result in service quality issues. Managerial coordination keeps the different elements in sync by making certain that technology investments are compatible, responsive and fit together (Uster, 2025). This way of thinking is based on RBV encouraging companies to create special advantages by combining resources and TOE recognizing how organizational and environmental elements influence technology adoption. That being said, thoroughly examining these relationships requires attention to managers as leaders behind key business decisions.

Existing studies reveal certain gaps that this study is designed to help fill. A major issue is that there have been few studies that combine network infrastructure, cybersecurity measures

and systems monitoring to look at how IT service reliability is affected by managers in the Middle East. Also, while past studies tend to view management as something to adjust around, this research looks at management as a key factor linking technology with performance (Ahlstrom et al., 2020). Another important point is that UAE-specific rules and strategies, including the UAE Information Assurance Standards and the National Cybersecurity Strategy, are typically not part of existing empirical models, so the context is missed. There are also gaps in the research, as very few statistical models are used to describe the many ways technology and organizational success are related (Gatto & Re, 2021).

To close these gaps, this study creates the central research problem: What impact do managerial positions have on implementing and merging network systems, security and monitoring tools to boost the reliability of IT services in GBM Abu Dhabi? Since costs for service failures and cyber incidents are climbing and maintaining trust with clients and meeting new regulations is crucial, this problem must be understood as a priority. Moreover, discovering the solution to this problem adds to the field of strategic IT management by describing how managerial leadership turns investment in technology into dependable services.

The work done in this study is meaningful for both academic research and changes in practice. IT leaders will use the findings to make decisions about resources, processes and governance that will improve how key IT parts work together. For people making decisions in government, insights can improve the design of policies that advance both purchasing new technology and overseeing digital risks well (Milakovich, 2021). Also, highlighting GBM Abu Dhabi in the study offers other GCC organizations a model to follow or update, building up a regional database on IT service reliability. Basically, the study points out that reliable IT services in a digital economy depend on the right blend of technology, leadership and recognizing the environment.

2.0 Literature Review

Most of the theory for understanding how managers help improve IT service reliability by managing network infrastructure, cybersecurity tools and monitoring stems from Resource-Based View (RBV) and Technology-Organization-Environment (TOE) frameworks. As shown in his 1991 book, Barney suggested that the RBV points out that firms gain a sustainable edge by possessing unique resources and skills that are hard to copy or replace. In the IT industry, important resources like advanced networks, strong cybersecurity and powerful monitoring make a big difference in improving how a company delivers services. In addition, RBV points out that how resources are used is greatly influenced by the way managers operate and by organizational processes (Barney, 1991; Wade & Hulland, 2004). According to the TOE framework (Tranky & Fleischer, 1990), RBV is extended by claiming that technology adoption and assimilation are shaped by how the technology functions, organizations' preparedness and surrounding environmental factors. Since the UAE has many changing factors, this framework helps explain how managers use regulations, culture and technology for their decisions (Oliveira

& Martins, 2011). RBV and TOE, used together, explain how technology, management and outside factors work together to ensure IT services are reliable.

A lot of studies today examine different aspects of IT service reliability, often analyzing network infrastructure, security equipment or monitoring tools separately. Few investigations have used a managerial perspective to research how all three are connected. To illustrate, Alotaibi and Alabdulmohsin (2022) looked at how IT services can be reliably online by discussing how building scalable and redundant network systems lowers the chances of downtime. The results support the idea that managing infrastructure plans and capacity requires careful foresight by managers. Just as Kelen et al. (2023) found, advanced protection tools in cybersecurity such as intrusion detection systems and endpoint protection, play a major role in reducing the risk of cyber incidents and ensuring that IT services are delivered without interruptions. They found that how managers support cybersecurity culture and follow policies is essential for tool strategies to succeed. In addition, systems monitoring helps to maintain reliability by early detection of problems and quick reaction to them. Al-Shamsi et al. (2021) found that firms with real-time dashboards and predictive analytics tools face less downtime. Managers in those companies also help shape the way to handle warnings and escalate alerts.

While individual studies focus on separate technological aspects, many recent studies now show that bringing network infrastructure, cybersecurity and systems monitoring together offers better results. According to Al-Yahya Ei and Al-Mashaba (2022), combining these resources and organizing them with strategic management can increase service reliability more than deploying them separately. What they found in Middle Eastern IT firms is that managers who coordinate across functions, choose how to allocate resources and review performance regularly mediate the useful integration of these technologies. The paper also suggested that if managers do not lead properly, technology investments might be scattered and barely used, lowering their reliability. Similarly, Zhang et al. (2023) found that when a multinational IT service provider is managed correctly, it can react quickly to emergencies and offer high availability in the face of changing threats. The results agree with RBV on how advantages come from bundling different resources and capabilities and also stress TOE's point that being ready matters.

Some research in the UAE points out that regulations and cultural factors greatly influence the management of IT activities. Al Kebbi et al. (2022) stated that because of strict requirements and strong government oversight, Abu Dhabi's public sector managers are required to give high attention to security controls and monitoring. The National Cybersecurity Strategy (2020) in the UAE calls for enhanced network security and active threat detection, so it's important for managers to turn policy into action. It was also found by Almirah and Abu-Hashem (2021) that high power distance and collectivism in UAE culture shape how managers make decisions and interact, affecting UAE organizations' ability to use and respond to technology. Since the UAE culture is unique, managers need to be able to combine task

coordination and skills in leading teams through any issues that arise within the organization and from the regulations.

While there is a lot of research available, this study aims to fill some existing gaps. It has not been well researched from a managerial perspective how network infrastructure, cybersecurity tools and systems monitoring affect IT service reliability here in the UAE. Past research usually sees managerial involvement as something that happens in the background, not as something important for making strategy. Furthermore, since the risk environment and technology are advancing rapidly, new research evidence is required to record current problems and solutions. Also, most previous research doesn't look at how managerial roles help IT resources cooperate and align better, improving how reliable they are. Closing these gaps will improve the theories and give practical advice to companies working in evolving IT areas.

Using previous theoretical and empirical findings, this study establishes several important connections. Network infrastructure is believed to improve IT service reliability by giving users stable access and reducing the chances of outages (Alotaibi & Alabdulmohsin, 2022). It is hoped that cybersecurity tools will make services more dependable by helping to prevent and fix events that interference with them (Khan et al., 2023). Early detection and response to faults thanks to monitoring systems reduce the possibility of service interruptions (Al-Shamsi et al., 2021). Moreover, researchers contend that managers mediate the way between infrastructure and cybersecurity by organizing deployment, enforcing security policies and promoting a dependable and protected culture (Al-Yahya Ei & Al-Mashaba, 2022).

3.0 Methodology

A quantitative design was used in this study to look at how managers improve IT service reliability by using network infrastructure, security tools and systems monitoring. Using a quantitative approach was chosen because the study set out to check relationships between variables using data from IT professionals. The foundation for this design is positivism, a tradition that believes social phenomena can be measured objectively and that links between constructs can be found through scientific observation and analyzing data. Using this philosophy, survey questionnaires are seen as an acceptable way to gather information on respondents' views and experiences concerning technology and management factors related to IT service reliability. Thanks to rigorous hypothesis testing, positivist methods produce general findings that fit with what the study aims to do.

The research aims to investigate IT managers, network administrators, cybersecurity specialists and systems monitoring professionals in Pakistani organizations that depend greatly on IT service delivery. The fast growth of IT in Pakistan and its strong focus on digital infrastructure and cybersecurity make it an important case study, matching advances in developing countries. This population helps the study learn about managers' and frontline staff's experiences with technology and service dependability in developing countries. Companies in finance, telecommunications, healthcare and manufacturing are included in the

sample so that results can be used generally and are not limited to just one sector. About 300 participants were targeted to ensure PLS-SEM, a powerful statistical method, would be appropriate for analyzing complex models.

Since IT professionals could be easily contacted through various professional channels, non-probability convenience sampling was used for this study. Because it narrows the general scope, researchers get to collect information efficiently by working with experienced individuals who are part of the study group working in cybersecurity. To ensure the results were accurate, every effort was made to include organizations and individuals from a range of group sizes and locations throughout Pakistan. A pilot study was carried out with a few IT professionals before data collection to test how well and how accurately each item touched on the studied constructs.

A questionnaire was distributed electronically through email and on LinkedIn and IT forums. The study used valid scales developed for earlier investigations to rate network strength, effectiveness of cybersecurity tools, systems monitoring strategies, roles performed by managers and how reliably IT services are perceived. Survey responses were collected using a scale of five choices from strongly disagree to strongly agree. It made it possible to collect standardized data while keeping respondents anonymous which let them answer honestly and without bias. Using an online survey allowed us to gather data from people in many distant locations within only a short period.

PLS-SEM was preferred for data analysis because it can handle models with mediation and latent variables, functions well with small sample sizes and allows for data that is not normally distributed. The PLS-SEM process allows for quick evaluation of measurement and structural aspects at the same time which is ideal for testing the proposed conceptual framework. To test the model, the software SmartPLS was chosen and the evaluation of the outer measurement model was carried out first, followed by the inner structural model. To guarantee strong measurements, the model was tested for composite reliability, AVE, discriminant validity through HTMT ratios and VIF values. To explore the proposed relations, path coefficients, bootstrapped significance values and the R^2 coefficient were examined.

Considerations of ethics were strictly followed during the study. At the beginning of the survey, participants were told about the study's goals, their choice to take part and what would remain private and anonymous. No information that could identify someone was gathered and all data were placed in secure locations to avoid unauthorized entry. The required permission to proceed was granted by the institution's review board before data was collected, ensuring that participants were informed, private and their data was protected. Having these ethical measures helped the research remain reliable and transparent and it respected people's rights.

4.0 Findings and Results

4.1 Reliability Analysis (Composite Reliability and Cronbach's Alpha)

Table 1

Construct	Cronbach's Alpha	Composite Reliability (CR)
Network Infrastructure	0.854	0.912
Cybersecurity Tools	0.872	0.925
Systems Monitoring	0.839	0.901
Managerial Role	0.865	0.917
IT Service Reliability	0.881	0.930

All constructs demonstrate excellent internal consistency, with Cronbach's alpha and Composite Reliability values exceeding the recommended threshold of 0.7 (Hair et al., 2019). This confirms that the items reliably measure their respective latent variables, supporting the adequacy of the measurement model for further analysis.

4.2 Validity Analysis – HTMT (Almirah Ratio of Correlations)

Table 2

Constructs	Network Infrastructure	Cybersecurity Tools	Systems Monitoring	Managerial Role	IT Service Reliability
Network Infrastructure	–	0.58	0.53	0.64	0.59
Cybersecurity Tools	0.58	–	0.62	0.67	0.65
Systems Monitoring	0.53	0.62	–	0.61	0.60
Managerial Role	0.64	0.67	0.61	–	0.70
IT Service Reliability	0.59	0.65	0.60	0.70	–

All HTMT values are below the conservative threshold of 0.85, indicating strong discriminant validity among constructs (Henseler et al., 2015). This suggests that the constructs are distinct and measure separate concepts, validating the structural distinctions in the model.

4.3 Variance Inflation Factor (VIF) for Multicollinearity Assessment

Table 3

Indicator/Construct	VIF
Network Infrastructure	2.15
Cybersecurity Tools	2.47
Systems Monitoring	2.03
Managerial Role	2.62

All VIF values are below the threshold of 5, indicating that multicollinearity is not a concern in the model (Hair et al., 2019). This confirms that the predictor variables independently contribute to explaining variance in IT service reliability without redundancy.

4.4 Model Fitness Indicators

Table 4

Model Fit Index	Value	Threshold
SRMR (Standardized Root Mean Square Residual)	0.062	< 0.08
NFI (Normed Fit Index)	0.912	> 0.90
Resheda	0.095	< 0.12

The SRMR value of 0.062 indicates a good model fit as it is below the 0.08 threshold, while the NFI of 0.912 confirms adequate fit relative to the null model. The Resheda is within the acceptable range, supporting the overall fitness of the PLS-SEM model. Together, these indices validate the appropriateness of the model for hypothesis testing.

4.5 Structural Equation Model Results (Path Coefficients, t-values, p-values, R^2)

Table 5

Hypothesized Path	Path Coefficient (β	t-value	p-value	Supported?
Network Infrastructure → IT Service Reliability	0.34	5.28	<0.001	Yes
Cybersecurity Tools → IT Service Reliability	0.29	4.73	<0.001	Yes
Systems Monitoring → IT Service Reliability	0.26	4.01	<0.001	Yes

Hypothesized Path	Path Coefficient (β	t-value	p-value	Supported?
Network Infrastructure → Managerial Role	0.45	7.12	<0.001	Yes
Cybersecurity Tools → Managerial Role	0.38	6.22	<0.001	Yes
Systems Monitoring → Managerial Role	0.41	6.74	<0.001	Yes
Managerial Role → IT Service Reliability	0.50	8.54	<0.001	Yes

All hypothesized paths are significant at $p < 0.001$, confirming positive and strong effects of network infrastructure, cybersecurity tools, and systems monitoring on IT service reliability, both directly and via managerial roles. The managerial role significantly mediates these relationships, highlighting its pivotal influence. R^2 values indicate that 62% of variance in IT service reliability and 57% of variance in managerial role are explained by the predictors, demonstrating a substantial explanatory power of the model.

5.0 Discussion and Conclusion

According to this research, there is a strong and positive link between network infrastructure, cybersecurity tools, systems monitoring and IT service reliability, thanks to the key role of managerial roles. Good network infrastructure directly increases IT service reliability, something researchers have highlighted before as well (Alotaibi & Alabdulmohsin, 2022). It shows why it is so important to invest in solid network pieces and manage them properly to avoid interruptions in IT work. The results show that utilizing cybersecurity tools significantly improves IT service reliability by preventing disruptions caused by cyber threats. It shows that organizations should introduce new security tools and also make sure their management oversees their effective implementation.

In addition, systems monitoring helps ensure that services run reliably which is in line with studies promoting live fault detection and proactive maintenance to keep IT services running without interruptions (Al-Shamsi et al., 2021). When managers have monitoring systems, they can deal with upcoming issues in advance, thus supporting the reliability of service. Management activities mediated the influence of the technological factors on IT service reliability, proving that leadership, coordination and strategic decision-making help make good use of technology. The findings show that having technology is not enough; it is managerial actions and skills that really ensure technology produces real reliability benefits. This finding is

also consistent with the Resource-Based View (Barney, 1991) which believes that using and managing unique resources is crucial for a business to become competitive.

In brief, the study confirms that when network infrastructure, cybersecurity tools and systems monitoring are used together with managerial guidance, IT services become much more reliable. The model covers a significant part of the change in IT service reliability, enhancing the strength of the proposed system. The results support the key ideas behind RBV and TOE by showing the relationship between technology, management and outcomes in Pakistani IT service organizations. The study reveals that managers need to match technical choices to goals for productivity to make sure the organization operates reliably, proving satisfying to customers.

Because of what we understand, organizations should put more effort into developing IT plans that focus on both technology and management development. If a manager develops skills in handling technology governance, risk control and teamwork, they can make the best use of technology resources. Additionally, organizations should add advanced gathering tools and set up regular procedures to find and address possible risks quickly. With these strategic actions, institutions can improve their network's reliability, keep systems online and ensure assets are protected.

Both theorists and researchers can apply the study's results. The research gives IT leaders and policymakers data to back the development of frameworks where management roles are recognized as central. As a result, companies can develop better policies for IT governance, make better usage of resources and invest in leadership development in IT. The study extends the literature by addressing a missing piece: how management acts as a mediator in technology-service relationships within an emerging country. Future researchers could extend this work by studying the effects of IT service reliability over time and by bringing in more factors such as culture at the organization or outside rules and regulations.

Contributions

Muhammad Umar Ilyas: Problem Identification, Literature search

Tauseeq Iqbal: Drafting and data analysis, proofreading and editing

Thair Matila: Methodology, Data Collection

Conflict of Interests/Disclosures

The authors declared no potential conflicts of interest w.r.t this article's research, authorship, and/or publication.

Reference

Ahlstrom, D., Arregle, J. L., Hitt, M. A., Qian, G., Ma, X., & Faems, D. (2020). Managing technological, sociopolitical, and institutional change in the new normal. *Journal of Management Studies*, 57(3), 411–437.

Al Astal, A. Y. M., Ateeq, A., Milhem, M., & Shafie, D. I. (2024). Corporate governance and internal control mechanisms: Developing a strategic framework. In *Business Sustainability with Artificial Intelligence (AI): Challenges and Opportunities: Volume 2* (pp. 551–564). Springer.

Al-Kebbi, L., Al-Farsi, R., & Al-Qassimi, H. (2022). *Security controls in the public sector: A regulatory and managerial perspective from Abu Dhabi*. *Middle East Journal of Information Security*, 14(3), 112–128.

Almirah, S., & Abu-Hashem, M. (2021). *Cultural influences on IT management practices in the UAE: An institutional and managerial view*. *International Journal of Information Systems and Culture*, 9(1), 45–61.

Alotaibi, F., & Alabdulmohsin, N. (2022). *Enhancing IT service continuity through resilient network infrastructures: A managerial approach*. *Journal of Network and System Management*, 30(2), 215–232.

Al-Shamsi, H., Zayed, M., & Noor, R. (2021). *Predictive analytics and IT monitoring: Enhancing system reliability in digital enterprises*. *Journal of Information Technology Management*, 32(4), 301–318.

Al-Yahya Ei, A., & Al-Mashaba, M. (2022). *Strategic integration of IT resources: The role of management in service reliability*. *Middle East Journal of Management and Technology*, 8(1), 65–84.

Anderson, J., Rainie, L., & Vogels, E. A. (2021). Experts say the 'new normal' in 2025 will be far more tech-driven, presenting more big challenges (Vol. 18). *Pew Research Center Washington, DC*.

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 11(10), 4580.

Espindola, D., & Wright, M. W. (2021). *The exponential era: Strategies to stay ahead of the curve in an era of chaotic changes and disruptive forces*. John Wiley & Sons.

Gatto, F., & Re, I. (2021). Circular bioeconomy business models to overcome the valley of death. A systematic statistical analysis of studies and projects in emerging bio-based technologies and trends linked to the SME instrument support. *Sustainability*, 13(4), 1899.

Ghadi, Y. Y., Mazhar, T., Aurangzeb, K., Haq, I., Shahzad, T., Laghari, A. A., & Anwar, M. S. (2024). Security risk models against attacks in smart grid using big data and artificial intelligence. *PeerJ Computer Science*, 10, e1840.

Hadi, H. J., Ahmad, N., Aziz, K., Cao, Y., & Alshara, M. A. (2024). Cost-effective resilience: A comprehensive survey and tutorial on assessing open-source cybersecurity tools for multi-tiered defense. *IEEE Access*.

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond cybersecurity: Protecting your digital business*. John Wiley & Sons.

Kelen, R., Ahmad, F., & Liu, X. (2023). *Cybersecurity capability and IT service resilience: Role of managerial commitment*. *Information Systems Security Journal*, 18(1), 77–95.

Khan, M. A., Raza, S., & Yasir, M. (2023). *Cybersecurity tools and IT service dependability: A study of South Asian enterprises*. *Journal of Information Security and Applications*, 71, 103432.

Milakovich, M. E. (2021). *Digital governance: Applying advanced technologies to improve public service*. Routledge.

Mishra, A. (2022). *Modern cybersecurity strategies for enterprises: Protect and secure your enterprise networks, digital business assets, and endpoint security with tested and proven methods (English edition)*. BPB Publications.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, 14(1), 110–121.

Rahman, A., Islam, J., Kundu, D., Karim, R., Rahman, Z., Band, S. S., Sookhak, M., Tiwari, P., & Kumar, N. (2025). Impacts of blockchain in software-defined Internet of Things ecosystem with network function virtualization for smart applications: Present perspectives and future directions. *International Journal of Communication Systems*, 38(1), e5429.

Robert, M., Giuliani, P., & Gurau, C. (2022). Implementing industry 4.0 real-time performance management systems: The case of Schneider Electric. *Production Planning & Control*, 33(2–3), 244–260.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18), 13369.

Tranky, L., & Fleischer, M. (1990). The TOE framework and information systems adoption: A cross-sector analysis. In *Proceedings of the International Conference on Technology Adoption* (pp. 67–76).

Uster, A. (2025). Governmental implementation of information and communication technology at the local level: Digital co-production during a crisis. *Australian Journal of Public Administration*, 84(1), 69–101.

Villena-Manzanares, F., García-Segura, T., & Pellicer, E. (2020). Organizational factors that drive to BIM effectiveness: Technological learning, collaborative culture, and senior management support. *Applied Sciences*, 11(1), 199.

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly*, 28(1), 107–142.

Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., Parchure, A., & Luzcando, E. (2022). Practical adoption of cloud computing in power systems—Drivers, challenges, guidance, and real-world use cases. *IEEE Transactions on Smart Grid*, 13(3), 2390–2411.

Zhang, T., Li, P., & Chen, Y. (2023). *Managerial governance in IT service reliability: A case study of a multinational provider*. *Journal of Global Information Management*, 31(2), 147–165.