



INTERNATIONAL JOURNAL OF
INNOVATION AND
INDUSTRIAL REVOLUTION
(IJIREV)

www.gaexcellence.com/ijirev



THE IMPACT OF DIGITAL TRANSFORMATION ON ORGANIZATIONAL PERFORMANCE IN UAE SECURITY AGENCIES: A QUALITATIVE SYSTEMATIC LITERATURE REVIEW

Khalfan Abdulla^{1*}, Rafiduraida Adulrahman²

¹Faculty of Management and Economic, Sultan Idris Education University, Malaysia

 K.uae.dxb@gmail.com

 <https://orcid.org/0009-0003-2897-7817>

²Faculty of Management and Economic, Sultan Idris Education University, Malaysia

 rafiduraida@fpe.upsi.edu.my

 <https://orcid.org/0000-0001-8225-188X>

*Corresponding Author

Article Info:

Article history:

Received date: 19.07.2026

Revised date: 11.08.2026

Accepted date: 10.09.2026

Published date: 28.09.2026

To cite this document:

Abdulla, K., & Adulrahman, R. (2026). The Impact of Digital Transformation on Organizational Performance in UAE Security Agencies: A Qualitative Systematic Literature Review. *International Journal of Innovation and Industrial Revolution*, 8(26), 807-825.

Abstract:

Digital transformation (DT) is a strategic priority for security agencies around the world, especially in the United Arab Emirates (UAE), where it serves as the foundation for the UAE National Cybersecurity Strategy and UAE Digital Government Strategy 2025. Yet, empirical studies of the experience and enactment of digital transformation in security institutions are still limited: direct access to serving security practitioners for academic research is highly restricted, and the literature generally on digital transformation in the UAE is mainly quantitative and survey-oriented, providing limited evidence of the situated, sense-making, and contested processes by which digital transformation actually works. Given these limitations, the present review will apply the principles of PRISMA reporting to conduct a qualitative systematic literature review (SLR) and thematic synthesis (Thomas & Harden, 2008) to analyse only those qualitative, empirical studies (case studies, in-depth interviews, focus groups, ethnographic or interpretive fieldwork, and qualitative document analysis) focused on digital transformation and organisational performance in security, policing, and other public-sector organisations with a strong regulatory requirement, complex operational environments, hierarchical structures, and high levels of responsibility for cybersecurity or digital-governance. There is limited UAE qualitative evidence in the review, so it also included other similar public sector security organisations from around the world to identify mechanisms transferrable to the UAE and to provide context to the limited evidence in the UAE. The database search itself resulted in 46 candidate records, which were further reduced to 40 after removing those that were duplicates, then through

screening by title and abstract, 10 primary qualitative studies were identified: 4 relating to UK policing, 4 relating to Dutch and Indonesian police organisations, 1 to Dubai Police, 1 to Indian public-health administration and 1 to public-sector Chief Digital Officers in several countries. The conclusions presented here are analytical and illustrative and cannot be generalized statistically as the evidence base is relatively small, and the empirical qualitative research on digital transformation in public-sector security organisations is limited. Thematic synthesis resulted in five descriptive themes which aligned with the five dimensions of digital transformation explored in this review (IT infrastructure/digital capability, cybersecurity integration, and digital leadership, workforce digital competency and e-service innovation), and three cross-cutting analytic themes: (1) digital transformation as a liminal, locally negotiated process rather than a discrete rollout; (2) leadership and culture, rather than infrastructure alone, as the mechanism linking technology to performance; and (3) the underrecognized role of frontline and mid-level personnel as adaptive performance drivers. Themes have direct implications for the leadership of UAE security agencies.

DOI: 10.35631/IJIREV.826048

Keywords:

Digital Transformation, Organizational Performance, Policing, Qualitative Research, Security Agencies, Systematic Literature Review, Thematic Synthesis, UAE



© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact ijirev@gaexcellence.com.

Introduction

Digital transformation (DT) is the integration of information, computing, communication, and connectivity technologies to create a paradigm shift in the way organizations are run. It has shifted the private sector to the center of government institutions (Vial, 2019). This is particularly evident in the UAE, where the use of technology is the core of national competitiveness and national security policy. A special case in this larger narrative is security agencies, such as police, civil defense, coast guard, and intelligence agencies: their effectiveness is not just gauged by their efficiency but by their own safety of the population, the confidentiality of their operations, and the trustworthiness of their institutions, and their staff is by policy rarely available to external academic researchers as primary data sources (Elnaghi et al., 2019).

Most of the known quantitative information regarding digital transformation and organizational performance in the context of the public sector and the UAE is based on survey-based, variable-centered research, regression, or structural equation modelling (Alhajeri, 2022). That literature can help set the direction and rough scale of relationships, but not to answer another, equally critical question: how does it go, in fact, in the context of an operating security institution, and how do people experience it? Qualitative studies such as case studies, interviews, ethnography,

and document-based institutional analysis are specifically structured to answer that question, and an accumulating literature in qualitative terms exists in the field of policing as well as other similar organizations in the public sector worldwide, although very little of the existing qualitative literature has been brought to bear explicitly in the context of the UAE security environment.

This review addresses such a gap. Instead of introducing another quantitative estimate, or trying to gather new primary data by interviewing UAE security personnel (which access limitations to current data would make impractical), it performs a qualitative systematic literature review (SLR): a search and synthesis informed by PRISMA reporting principles, of already-published, peer-reviewed studies that utilized qualitative empirical methods - case study, interview, focus group, ethnographic or qualitative document-analytic methodology - to study digital transformation and organizational performance in security, policing, and closely related public-sector contexts (Alzarooni et al., 2024). It is not intended to estimate an effect size, but to find out what processes, tensions, and mechanisms recurrently emerge through digital transformation, encountering operational, rule-bound, high-accountability institutions, which are the same features of institutions that define UAE security agencies.

Early UAE-oriented scholarship on this subject in itself is educative on this point. In a case study of the service re-engineering of Dubai Police, Elnaghi et al. (2019) based their analysis on interviews and document analysis of the transformation process, as opposed to a survey tool, discovered that the role of the government authority in managing the change process, as opposed to merely funding the technology, was decisive in whether re-engineering would lead to lasting performance improvements. Such a process-level understanding is structurally inaccessible to a cross-sectional survey design, and it is precisely the type of understanding that this review aims to comprehensively collect and compile over a broader international qualitative literature.

The traditional version of digital transformation in security institutions is characterized by a number of interacting dimensions: (1) IT infrastructure modernization and digital capability (ITIM), (2) cybersecurity integration (CSI), (3) digital leadership (DL), (4) workforce digital competency (WDC), and (5) e-service innovation (ESI). This review keeps these five dimensions as a structure to organize the thematic synthesis, but it is open to cross-cutting themes that cannot be well mapped on to any one dimension - something that qualitative synthesis is, once again, well placed to bring to light compared to quantitative synthesis using variables.

Research Objectives

1. To study the experience and practice of IT infrastructure modernization and digital capability (ITIM) in security and public-sector entities, based on the qualitative literature.
2. To explore the organizational and human processes that qualitative studies find to influence cybersecurity integration (CSI) in practice.
3. To establish, based on the qualitative literature, the extent to which digital leadership (DL) plays in enabling organizational performance due to digital transformation.
4. To assess the qualitative nature of workforce digital competency (WDC) development and implementation in the environment of operational institutions in the public sector.

5. To identify what qualitative descriptions of e-service innovation (ESI) can tell us about its association with internally perceived organizational performance, in comparison with externally perceived service quality.

Research Questions

Because this is a qualitative synthesis rather than a hypothesis-testing study, the review is guided by research questions rather than directional hypotheses:

- RQ1: What is the experience and implementation of IT infrastructure modernization and digital capability (ITIM) in security and public-sector organizations, based on the qualitative literature?
- RQ2: What are organizational and human processes that a qualitative study finds to influence cybersecurity integration (CSI) in practice?
- RQ3: What does the qualitative literature determine the role and boundaries of digital leadership (DL) in facilitating the performance of organizations as a result of a digital transformation?
- RQ4: What are the qualitative characteristics of workforce digital competency (WDC) development and application within the context of operational institutions in the public sector?
- RQ5: What can qualitative descriptions of e-service innovation (ESI) tell us about how it is related to internally perceived organizational performance, as compared to externally perceived service quality?

Literature Review

Methodology

Research Design

This study is a qualitative systematic literature review (SLR). It does not gather new primary data on UAE security staff or any other human participants; rather, it implements a structured search protocol, guided by PRISMA reporting guidelines by Moher et al. (2009), to locate already published, peer-reviewed research which in turn employed qualitative empirical methods, and synthesizes its results through thematic synthesis (Thomas and Harden, 2008), a methodology formulated to synthesize results across multiple qualitative primary studies in systematic reviews. This approach is part of a historical and current tradition of qualitative evidence summary in the study of public administration and information-systems and is distinct and not reducible to meta-analysis of quantitative effect sizes.

Search Strategy and Databases

A Boolean string was used to search the title, abstract and keyword fields of Scopus and major publisher databases (ScienceDirect, SpringerLink, Taylor & Francis Online, MDPI journals, Emerald Insight and Google Scholar) for transformation terms ("digital transformation" OR digitalization OR digitalisation), setting terms (police OR policing OR "security agency" OR "public sector" OR "government organization") and qualitative methodology terms (case study OR interview OR ethnograph* OR "thematic analysis" OR "grounded theory" OR qualitative).

The search was conducted from January 2015 to June 2026 in English and completed in June 2026. Peer-reviewed journal articles in English were only included for screening.

Inclusion and Exclusion Criteria

The inclusion criteria in this review combine an organisational-scope boundary with a methodological one. Organisationally, eligible studies had to be conducted within a security agency, policing organization, or another public-sector organisation sharing the defining characteristics of that setting high regulatory requirements, complex operational environments, hierarchical structures, and significant cybersecurity or digital-governance responsibilities. This is why, alongside policing and security-agency studies, the review also admits studies of public-sector Chief Digital Officers and of a public-health administration whose accountability structures, hierarchical governance, and digital-governance responsibilities meet this same boundary, even though they are not security agencies in the narrow sense. Methodologically, all sources included in the review should describe empirical research that included a qualitative research design - case study, semi-structured or in-depth interviews, focus groups, ethnographic or interpretive fieldwork, grounded theory, or qualitative (thematic or content) document analysis. Purely quantitative studies (survey-based regression, SEM, or PLS-SEM with no qualitative component) were not considered at all, nor were mixed-methods studies in which the qualitative component could not be separated from the quantitative results. This is a purposefully more limiting criterion than many public-sector digital-transformation reviews would have, and it severely limited the quantity of otherwise-relevant UAE-specific sources that could be found, as most of the extant literature on UAE-specific digital-transformation is survey- and PLS-SEM-based, as opposed to qualitative as demonstrated in table 1 below.

Table 1: Inclusion and Exclusion Criteria

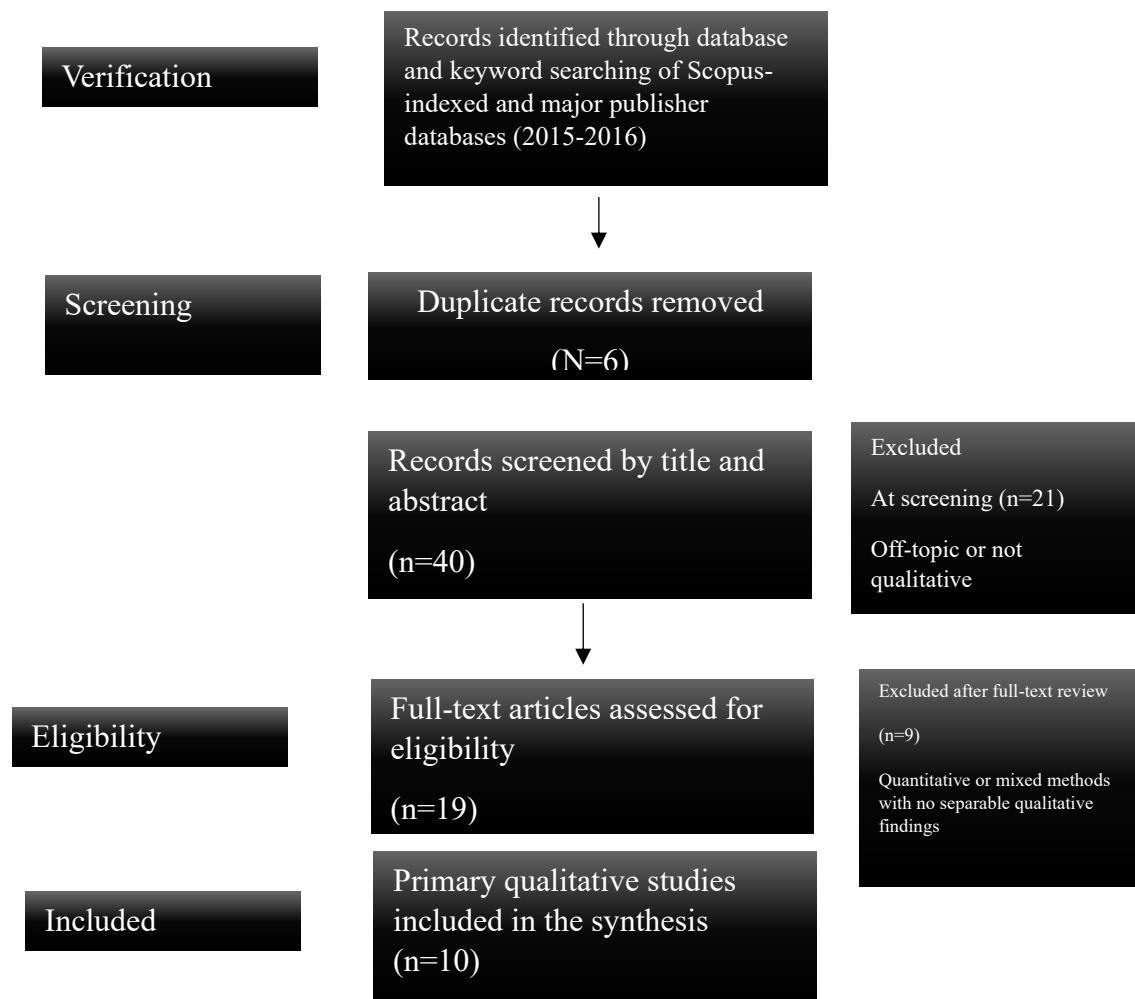
Inclusion Criteria	Exclusion Criteria
Peer-reviewed journal article, 2015–2026, English language	Books, theses, non-peer-reviewed working papers
Empirical research based on a qualitative research methodology (case study, interview, focus group, ethnography, grounded theory, or qualitative document/content analysis) Purely quantitative designs (survey-regression, SEM, PLS-SEM) with no qualitative element.	Purely quantitative designs (survey-regression, SEM, PLS-SEM) with no qualitative component
Addresses digital transformation, digitalization, or a specific DT dimension (ITIM, CSI, DL, WDC, ESI) in relation to organizational performance, change, or outcomes	Mixed-methods studies in which qualitative findings cannot be isolated from quantitative results
Conducted within a security agency, policing organization, or a public-sector organization with comparable operational, rule-bound, or high-accountability characteristics	Purely conceptual or theoretical papers with no empirical qualitative data collection or analysis
Sufficient methodological transparency to identify data source, sample/informant	Studies with no discernible or reported qualitative analytic procedure

Inclusion Criteria	Exclusion Criteria
characteristics, and analytic approach (e.g., thematic analysis, grounded theory coding)	

Study Selection

Following PRISMA reporting principles, database and keyword searching identified 46 candidate records. 6 were removed for being duplicates and 40 were screened by title and abstract, of which 21 were removed because they were off-topic or not of a qualitative design. The remaining 19 records were retrieved and evaluated in full text, with nine records being excluded at this stage – mostly due to the fact that the approach of these records, on closer inspection, was quantitative or mixed method with a quantitative component that could not be separated from the qualitative findings, including a number of otherwise topical UAE public-sector studies of digital transformation. This process led to 10 main studies that met the eligibility criteria of the qualitative methodology; these form the coded corpus for thematic synthesis that is presented (Figure 1).

Figure 1: Prisma Flow Diagram



Thematic Synthesis Procedure

In line with the three-step approach of thematic synthesis of qualitative research suggested by Thomas and Harden (2008) when conducting a systematic review, this study followed: (1) line-by-line coding of the findings, results, and discussion sections of each of the included studies, where statements, illustrative interview material (paraphrased in this review, as opposed to direct quoting, in compliance with the limitations of reproducing another author original text), and reported observations related to the five dimensions of the DT were extracted; (2) sorting of these codes into descriptive themes based on patterns that remained close to the content of the individual primary studies; and (3) formation of analytical themes that transcend the content of the individual primary studies to generate new interpretive insight pertaining to the research questions of this review - in this case insight being particularly oriented to the UAE security-agency context. This is done through the same general logic as thematic analysis of Braun and Clarke (2006), but applied, however, across, and not within, a group of primary qualitative studies.

Quality Appraisal

All studies included were evaluated according to the Critical Appraisal Skills Programme (CASP) Qualitative Research Checklist (2018), which focused on the clarity of the research aim, the appropriateness of the qualitative research methodology, the sufficiency of the research design, the recruitment plan and data collection, reflexivity, ethics, the rigor of data analysis, the clarity of the findings, and the value of the research. All of them met the core CASP criteria and appraisal comments noted that the results of some research (such as single organisation type case studies) are likely to be contextually specific rather than generalizable - a failing which is not fatal to CASP as appraisal but is recognised as a possible source of insight, as is the case in conventional qualitative evidence synthesis.

Findings

Table 2 summarizes the ten qualitative studies retained for thematic synthesis.

Table 2: Included Qualitative Studies

Study	Country / Context	Organization Type	Qualitative Method	Primary DT Dimension(s)
Elnaghi et al. (2019)	UAE	Dubai Police	Case study; interviews and document analysis of a government authority managing service re-engineering	ESI; DL
Gritt et al. (2024)	United Kingdom	UK policing	13-month interpretive case study (Klein & Myers, 1999); multi-source qualitative data	ITIM; DL
Fest et al. (2023)	Netherlands	Netherlands Police	Qualitative interview study of "data professional" system-level bureaucrats	ITIM; WDC

Alshaikh (2020)	Australia	Three large organizations (cybersecurity managers)	Interpretive multiple case study; semi-structured interviews, sentence-level coding	CSI
Ushaka Adie et al. (2024)	Multi-country (scoping review)	Public-sector organizations	Scoping review; thematic analysis of qualitative and conceptual digital-leadership literature	DL
Fannur (2025)	Multi-country	Public administration	Qualitative study of leadership themes: digital media, community, flexibility, professionalism	DL
Guenduez et al. (2025)	Multi-country	Public-sector organizations (25 Chief Digital Officers)	Semi-structured interviews; qualitative coding with supplementary structural topic modelling	ITIM; DL; ESI
Alamri et al. (2025)	Indonesia	Gorontalo City Resort Police	Descriptive qualitative case study; interviews with 8 purposively sampled informants; document review	WDC
Thakur et al. (2025)	India	Sub-district public-health administration	8 in-depth interviews; Braun & Clarke thematic analysis	WDC; ITIM
Listianto (2025)	Indonesia	East Java Regional Police (Cybercrime Directorate)	Qualitative empirical study; 12 informants; thematic analysis	ITIM; WDC

Table 3 quantifies the distribution of the ten studies included across the five dimensions of digital transformation before turning to each of the dimensions in the narrative detail, and Table 4 overlaid each study on the dimension/s that each study tackles. Due to multiple studies addressing more than one dimension, the most prominent being Guenduez et al. (2025) and Elnaghi et al. (2019), the number of dimensions in Table 3 is above ten.

Table 3: Frequency of Digital-Transformation Dimensions Across the Corpus

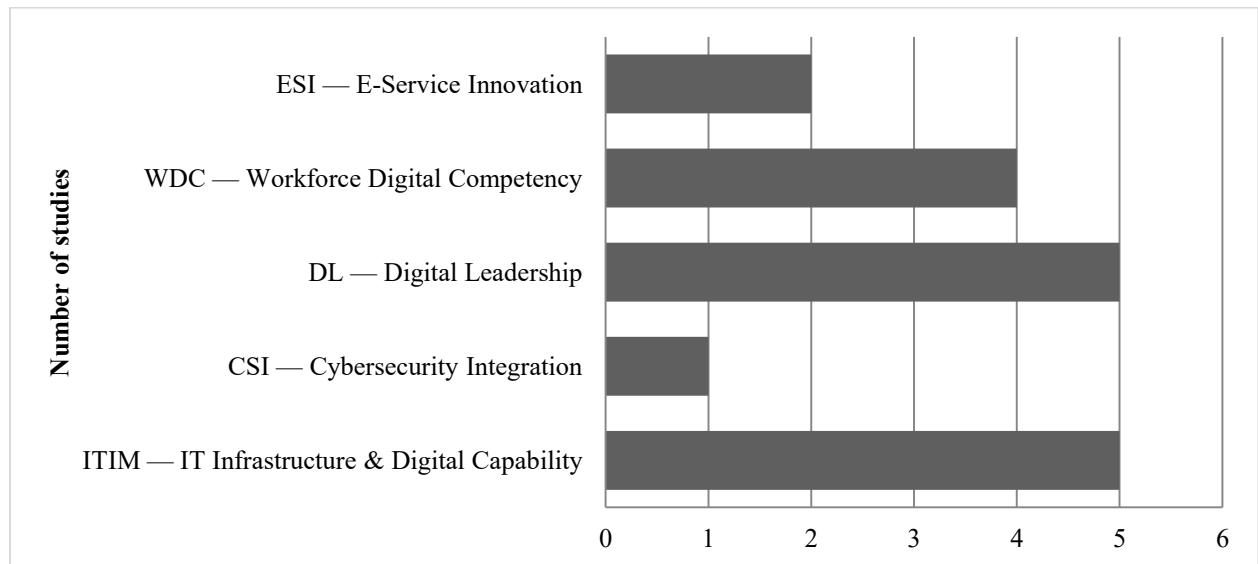
DT Dimension	Studies Addressing It	Share of Corpus (n=10)
ITIM — IT Infrastructure & Digital Capability	5	50%
CSI — Cybersecurity Integration	1	10%
DL — Digital Leadership	5	50%
WDC — Workforce Digital Competency	4	40%
ESI — E-Service Innovation	2	20%

Table 4: Study-by-Dimension Mapping Matrix

Study	ITIM	CSI	DL	WDC	ESI	Total
Elnaghi et al. (2019)	0	0	1	0	1	2
Gritt, Forsgren & Pandza (2024)	1	0	1	0	0	2
Fest et al. (2023)	1	0	0	1	0	2
Alshaikh (2020)	0	1	0	0	0	1
Adie, Tate & Valentine (2024)	0	0	1	0	0	1
Fannur (2023)	0	0	1	0	0	1
Guenduez et al. (2025)	1	0	1	0	1	3
Alamri, Kamuli & Abdussamad (2025)	0	0	0	1	0	1
Thakur et al. (2025)	1	0	0	1	0	2
Listianto (2025)	1	0	0	1	0	2
Total studies	5	1	5	4	2	17

Cells shaded indicate the key dimension(s) of a study. As indicated by the matrix, ITIM and WDC are often co-occurring (Fest et al., 2023; Thakur et al., 2025; Listianto, 2025), which is also in line with the descriptive theme, developed in Section 3.1 and 3.4, that infrastructural factors have an indirect effect on performance, through their impact on the adaptive capability of personnel.

Figure 2: Studies Addressing Each DT Dimension



ITIM: IT Infrastructure Modernization and Digital Capability

Through the literature on infrastructure and digital capability, one descriptive theme that is repeated is that, even though members of an organization can experience infrastructure investment, it is not as a singular, finished action but as a continuous, unresolved process. The 13-month interpretive case study of UK policing by Gritt et al. (2024) concluded that digital transformation in a police organization can be best described as liminal (incomplete, contested,

and negotiated locally) due to the openness of strategic direction, ambiguity in official rules, and cross-organizational interdependencies, which meant that the infrastructure changes were constantly renegotiated in everyday practice without settling in a new stable configuration. This makes it directly tricky to make any assumption that the investment in infrastructure translates easily or automatically into better performance.

Another similar theme based on the qualitative study of the Netherlands Police by Fest, Schaefer, van Dijck and Meijer (2023) is that a new digital infrastructure introduces new organizational positions and responsibilities - in their case, the introduction of new categories of system-level bureaucrats, such as data professionals, as a different category of discretionary power and accountability that does not suit the existing organizational structures. Their interview data revealed that these data professionals frequently knew the consequences of their technical efforts to the public-value and deployed different framing tactics to avoid being directly associated with the consequences, which the authors argue undermines the association between infrastructure capability and responsible performance improvement. The qualitative research of the Cybercrime Directorate of the East Java Regional Police reported by Listianto (2025) equally revealed that IT capability acts as a facilitator of dynamic capabilities -i.e. the role of infrastructure to affect organizational change is indirect and occurs through its impact on the ability to adapt and respond of personnel, but not directly as a performance driver itself.

CSI: Cybersecurity Integration

The most evident and stable qualitative theme of cybersecurity integration is the interpretive multiple-case study of Alshaikh (2020) of the managers of cybersecurity-awareness in three large organizations. Interpretation of interview data by sentence-by-sentence coding found that organizations that went beyond minimal policy compliance to a true security-first culture did so via five practices that recurred: identification and naming of specific target security behavior, creation of a network of peer security champions, who are embedded throughout business units, active branding and marketing of the internal cybersecurity service, the creation of a special engagement hub, and a deliberate alignment of security-awareness communication with the existing internal and external communications programs. One of the key themes of the research is that cybersecurity integration is a cultural and communicative accomplishment, rather than a technical one - the technology itself was found by participants to be necessary but inadequate, and organizational culture-building practice to transpose technical capacity into a consistent employee behavior and, by extension, organizational defense.

DL: Digital Leadership

The most widely theorized aspect of the studies included turned out to be digital leadership, but it is also the aspect where the qualitative literature becomes the most open on the boundaries of leadership. The scoping review by Ushaka Adie et al. (2024) based on thematic analysis of existing qualitative and conceptual literature on the topic structured the results into conceptual areas related to defining what digital leadership is, what the theoretical foundations of it are, and what specific competencies (vision, technical fluency, and ability to implement change in organizational culture) make it stand out among traditional leadership. One of the themes they share in their synthesis is that the digital leadership of the public sector is constrained in unique ways that are absent in the description of the same construct in the private sector, such as resource limits, competing political pressures, and structural inertia.

The interview study by Guenduez et al. (2025) of 25 Chief Digital Officers in the public sector confirms this image directly based on the first-hand experience of the practitioners themselves: their qualitative analysis revealed that the so-called persistence of innovation, or the long-term integration of innovation into the organizational culture and structure, or in other words the implementation of technology one-time projects, but not infrastructural, is the strategy that is explicitly reliant on the continued attention of the leadership and cultural transformation work, and not necessarily on the procurement of infrastructure. The account of one Chief Digital Officer, who participated in the study, described their work as leading employees in the transformation process and making sure that every other team is aligned so that the otherwise disconnected teams are aligned - a description which foreshadows the orchestration and sense-making work over technical execution. A qualitative study of public administrators by Fannur (2025) also found the same leadership themes as the most important ones that practitioners themselves emphasized, along with the presence of real obstacles to a transformation effort, which digital media literacy and community engagement alone, no matter what leaders may have intended them to be, could overcome, namely resistance to change, uneven digital literacy, and lack of resources;

The case study of Dubai Police by Elnaghi et al. (2019) can also be viewed as a direct and, more precisely, UAE-specific piece of information on this theme: it discovered that the active, ongoing management of the change process by the government authority, not its initial sponsorship of the technology, was the determinant of whether service re-engineering leads to long-term performance improvement. This is in line with the larger cross-national trend in the synthesized literature: the contribution of leadership to performance is real but seems to draw on the sustained cultural and process work, rather than initial decision or investment.

WDC: Workforce Digital Competency

Themes of workforce digital competency focus on the way employees develop and practice digital capability within the real limits of organizations, and usually informally. The qualitative case study of the Gorontalo City Resort Police by Alamri et al. (2025) (interviews with eight purposively sampled informants and analysis of strategic documents) revealed that enhancement of human-resource competence - such as predictive-analytics-based early-warning systems and competency-oriented training - was directly related by the informants to the department ability to reduce and solve crime, but also that budget constraints and internal opposition to more transparent, technology-infused work practices were some of the longstanding barriers to transferring individual competency improvements to overall performance.

The in-depth interview research by Thakur et al. (2025) of Indian sub-district public-health officers provides an especially rich description of adaptive agency: officers stated that they valued digital tools because of the transparency and real-time monitoring they facilitated, but also reported systemic constraints including hardware deterioration, poor connectivity, disjointed platforms, and limited fiscal autonomy that they maneuvered around through informal infrastructures like messaging applications, peer mentoring and parallel manual record-keeping. This informal adaptive work is one of the most conceptually important findings of the authors in the context of security-agency settings: the role of frontline and mid-level employees is presumably analogous in terms of enabler of organizational resilience, due to the meso-level work they perform. This is supported in the research by Listianto (2025) on the personnel of Indonesian cybercrime-unit who discovered that the IT proficiency of individual

officers was an organizational capability on its own, and not dependent on or supplementary to the formal technology infrastructure offered by the department.

ESI: E-Service Innovation

Themes of e-service innovation remain relatively underdeveloped in terms of the included qualitative corpus but reach a common conclusion: qualitative descriptions refer to internal organizational commitment, but not to the service-facing technology itself, as the constraining factor of whether e-service innovation will result in better performance. A case study of Dubai Police by Elnaghi et al. (2019) concluded that the continued internal dedication to the re-engineering process through coordination, overcoming resistance, and sustaining momentum post-initial launch of the service-innovation effort by the government authority, rather than the type of service technology used, was the difference between successful and stalled service-innovation initiatives. The interview data of Guenduez et al. (2025) also makes a similar distinction: between incremental innovation (digitizing and optimizing existing services) and transformational innovation (reconfiguring the underlying service-delivery model and internal organizational structure), with their Chief Digital Officer informants suggesting that the latter is significantly more reliant on the sustained internal cultural and structural change than the visible, citizen-facing technology itself.

Cross-Cutting Analytical Themes and Discussion

In addition to the five dimension-specific results, thematic analysis of the entire corpus identified three cross-cutting analytical themes that no single study included in it alone reports, which is consistent with the analytical (as opposed to a more descriptive) phase of the Thomas and Harden (2008) approach.

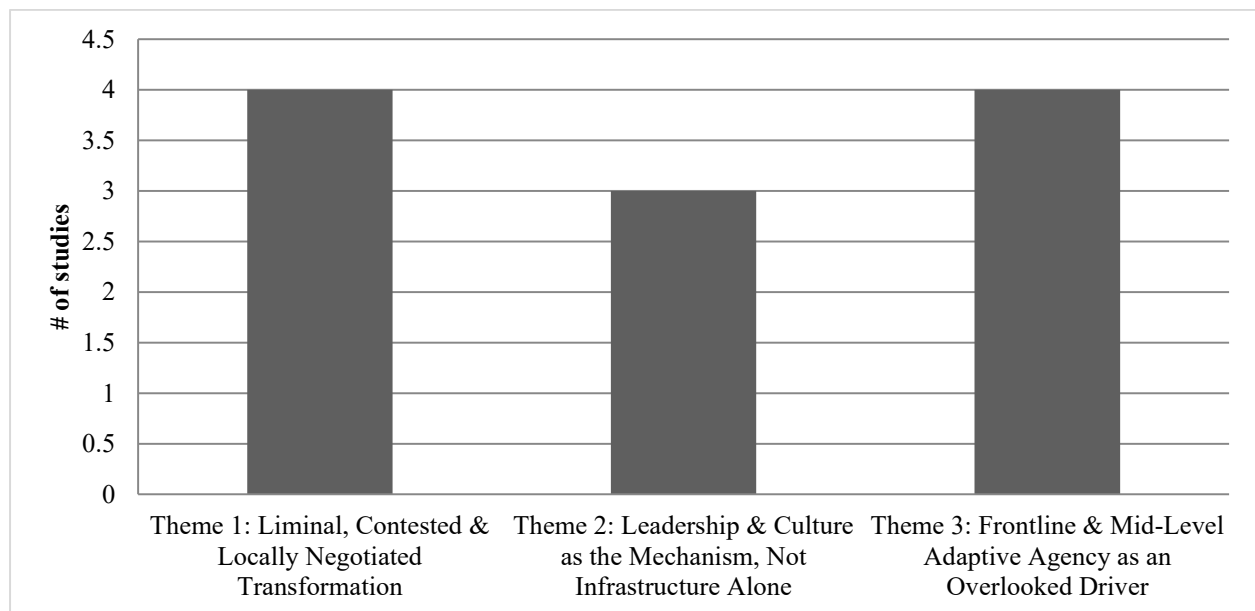


Figure 1: Supporting-Study Count per Cross-Cutting Theme

Theme One: Digital Transformation as Liminal, Contested, and Locally Negotiated

The most obvious cross-cutting theme is that the digital transformation within the rule-based, high-accountability public institutions is seldom a smooth, finished process of transition between an old and a new form of working. The idea of liminality (incomplete, contested, and localized transformation) presented by Gritt et al. (2024) is directly relevant to the observation by Fest et al. (2023) that new positions in the digital economy (data professionals) introduce a gray area of responsibility that cannot be clearly assigned by existing organizational structures and is not necessarily supplanted by the other. To UAE security agencies, this theme implies that digital transformation projects must be designed with the presumption of a long, actively managed transition period of simultaneous operation and localisation, not as a discrete implementation with an endpoint date - a planning assumption that is literally in line with what Elnaghi et al. (2019) found to differentiate between durable transformation and stalled transformation at Dubai Police specifically.

Theme Two: Leadership and Culture as the Mechanism, Not Infrastructure Alone

The qualitative literature across the CSI, DL, and ESI results, in specific, are united around a theme that infrastructure and technology serve as necessary and not sufficient conditions to improve performance - the specific mechanism, in nearly all of the studies included, is leadership behavior, cultural change work, or communicative/relational activity. The fact that cybersecurity culture is established not by technology implementation but by champion networks, branding, and communication campaigns (Alshaikh, 2020); the concept of persistent innovation (clearly, based on sustained leadership and embedding the culture) presented by Guenduez et al. (2025); the fact that the change process management (not technology sponsorship) at Dubai Police proved decisive (Elnaghi et al., 2019) all speak in the same direction. It is a significantly different focus than what a strictly quantitative, infrastructure-based survey instrument would tend to bring out, and it calls on UAE security-agency digital-transformation strategy to prioritize, among other things, leadership development, internal communications, and culture-change resourcing, as much as it prioritizes technology procurement.

Theme Three: Frontline and Mid-Level Adaptive Agency as an Overlooked Performance Driver

The third theme, which is most evident in Thakur et al. (2025) and Fest et al. (2023), but appears in a number of studies, is that frontline and mid-level staff have a large informal, adaptive agency in making digital systems work in practice - agency not usually foreseen or considered in formal documents of digital strategy. The meso-level health officers of Thakur et al. (2025) developed informal peer-mentoring and messaging-based workarounds to address infrastructure inadequacies; the police informants of Alamri et al. (2025) found competency-based training and predictive-analytics tools to be tailored by unit-level staff to the realities of their local operations, not applied uniformly top-down; and the informants of the cybercrime-unit of Listianto (2025) found organizational IT capability to be concentrated in the accrued proficiency of individual officers, and not necessarily applied uniformly across the top. According to this theme, the digital transformation of UAE security-agency performance can be as contingent upon the identification, resource mobilization of resources, and institutionalization of this first-line adaptive capacity as it is on any centrally planned system

or leadership initiative - a facet of organizational performance that a quantitative, top-down survey design is structurally less likely to identify.

Implications for the UAE Security-Agency Context

Combined, these themes indicate a tentative, qualitatively based framework of how digital transformation may be expected to impact organizational performance in UAE security agencies, pending direct primary qualitative research in those institutions, in particular. The case study by Elnaghi et al. (2019) of the Dubai Police is the only qualitative resource that is UAE-specific, but it remains consistent with all three cross-cutting themes: it recognizes long-term, proactively enforced organizational commitment, that is not the first choice of technology, as the determinant of service re-engineering, the same theme that the leadership-and-culture theme and the liminality theme identified in the broader international corpus. This overlap between the single UAE-specific qualitative source and the wider international qualitative literature is promising to the external validity of this synthesis, but it also highlights the paucity of the UAE-specific qualitative empirical research base: this review could only locate one qualitative empirical study carried out specifically in a UAE security institution.

Limitations

There are a number of limitations to this review which must be taken into account when interpreting the results. Firstly, and most fundamentally, the qualitative-methodology inclusion criterion, which is necessary in terms of a methodological justification of the purpose of the review, significantly narrowed the range of potential available evidence on the topic of the UAE, since the majority of current UAE-specific studies of public-sector and security-related digital-transformation are quantitative survey and PLS-SEM studies, and as such, were not included, irrespective of whether or not they were topical. The one UAE-specific qualitative source incorporated by Elnaghi et al. (2019) cannot, by itself, determine that the cross-national themes found here are applicable to the current UAE security-agency environment, especially given that it was published even earlier than some of the more recent UAE digital-government projects.

Second, by definition, qualitative case studies are contextually limited: the results of UK policing (Gritt et al., 2024), Dutch policing (Fest et al., 2023), or Indonesian policing (Alamri et al., 2025; Listianto, 2025) represent the situation in those institutions, under legal and cultural circumstances, and generalizability to the context of UAE security has not been directly experimented.

Third, thematic synthesis is also a process that requires interpretive judgment on the side of the reviewer in the process of identifying and naming both descriptive and analytical themes; although this review took the established procedure by Thomas and Harden (2008) and evaluated the included studies in accordance with the CASP (2018) checklist, a different synthesis team working on the same ten studies would reasonably arrive at somewhat different or more heavily top-ranked themes.

Fourth, the search, though systematic and guided by PRISMA, was in any case limited by access to databases and search-term selection; it is plausible that other potentially relevant qualitative studies, especially those that are unpublished institutional reviews or grey literature

within the UAE government agencies, are present but not identified by the protocol used in this review.

Conclusion

This qualitative systematic literature review aimed to learn, via thematic synthesis of other existing qualitative studies, the relationship between digital transformation and organizational performance in security agencies and similar close analogs in the public sector, without gathering new primary data of UAE security personnel. Ten qualitative studies, including UK, Dutch, Indonesian, Indian and UAE policing and public-sector settings, were synthesized into five dimension-specific descriptive themes and three cross-cutting analysis themes: digital transformation as liminal and locally negotiated over complete and linear; leadership and culture, over infrastructure alone, as the channel through which technology translates into performance; and frontline and mid-level adaptive agency as a performance driver underrecognized but with significant consequences.

These themes provide a qualitatively grounded, process-based complement to the already available quantitative literature on digital transformation and performance - a literature that, by design, is incapable of estimating the strength of that relationship at the scale that a quantitative study is capable of. The single, UAE-specific source in question by Elnaghi et al. (2019) aligns with the general synthesis, but the UAE-specific evidence base of qualitative evidence, in general, is still meager, so the UAE-specific central conclusion of this review is, in turn, a call to fill in this gap directly, with the help of case-study and interview-based research carried out within their respective institutions, informed by the themes and analytic framework presented in this review.

Recommendations

1. Architect digital transformation plans to be run over a long, proactively managed, period of parallel (digital and manual) operation. The theme of liminality (Gritt et al., 2024; Thakur et al., 2025) indicates that viewing transformation as a date-based rollout, as opposed to a long-term change-management process, poses a risk of not addressing the informal workarounds and unresolved role ambiguity - precisely what Elnaghi et al. (2019) identified to be the difference between durable and stalled transformation at Dubai Police.
2. No less than technology procurement is resource leadership and culture-change work. In the framework of CSI, DL, and ESI themes, qualitative literature tends to highlight leadership behavior and cultural embedding rather than the technology itself as the driver between digital investment and performance (Alshaikh, 2020; Guenduez et al., 2025).
3. Formally recognize and resource frontline and mid-level adaptive capacity. These personnel adaptive capacity to construct informal workarounds and locally adapted competencies indicates that UAE security agencies must view it as something to surface and support, not a form of informal deviation to be done away with (Alamri et al., 2025; Listiano, 2025; Thakur et al., 2025).
4. Demystify responsibility of new digitally enabled positions. The ambiguous responsibility of data professional roles identified by Fest et al. (2023) indicates that UAE security agencies launching similar data-intensive roles (e.g., analytics or

predictive-policing units) ought to establish discretion, responsibility, and public-value accountability of such roles proactively instead of this being negotiated informally.

5. Spend on cybersecurity culture-building activity, in particular, rather than technical controls. The five practices proposed by Alshaikh (2020) behavior identification, champion networks, internal branding, engagement hubs, and campaign alignment are a direct, evidence-based template.

Future Research

The most significant and evident research requirement that this review would bring out is face-to-face, primary qualitative research work in the field, within UAE security agencies per se, where operational security and classification will allow it, to determine whether the cross-national themes identified here (liminality, leadership-and-culture-as-mechanism, and frontline adaptive agency) are actually being realized by the UAE security situation, or whether the centrally mandated, resource-based model of digital transformation is yielding a qualitatively distinct pattern. In cases where access by full personnel is impractical, researchers could contemplate qualitative document analysis of UAE-security-agency digital-strategy documents, after-action reports, or training-materials, as part of the lower-access-barrier (though it still produces genuinely qualitative, process-level) part of the methodology of Elnaghi et al. (2019) and Alamri et al. (2025), under the same label.

Second, as this review identified a single study that was UAE-specifically focused (qualitative), it is apparent that UAE-based researchers have a chance to conduct a comparative qualitative case study of several UAE security agencies (police, civil defense, coast guard), applying the multiple-case-study design of Alshaikh (2020) to determine whether the theme of leadership-and-culture found in this review is consistent across the different types of security agencies or differ based on the institutional mandate.

Third, future qualitative studies may be more focused on examining the question of accountability and discretion that the concept of data professional introduces by Fest et al. (2023) in the context of UAE security agencies due to the swift expansion of data-analytics and AI-enabled capabilities in the field.

Lastly, a longitudinal qualitative study, such as pursuing a single UAE security-agency digital-transformation initiative throughout a long duration, as in the 13 months of the Gritt et al. case study (2024), would be especially suitable to directly test the liminality theme and to yield results that might be eventually triangulated with the quantitative evidence base to create a more comprehensive, mixed-methods view of how digital transformation impacts the performance of organizations in this industry.

-
- Acknowledgements:** The authors would like to express their sincere gratitude to Sultan Idris Education University, Malaysia, for providing the necessary resources and support throughout the course of this research. Colleagues and peers who provided enormous input and constructive feedback are highly appreciated, as they provided a significant improvement to the quality of this paper.
- Funding Statement:** No Funding
- Conflict of Interest Statement:** The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Innovation and Industrial Revolution (IJIREV).
- Ethics Statement:** No human subjects, animal subjects, or sensitive information were used in this research and therefore did not need ethical consent as it is a qualitative systematic literature review solely grounded on research work performed in the past. The authors affirm that the analysis was carried out following the established academic integrity and principles in ethics in publication.
- Author Contribution Statement:** Both authors contributed significantly to this manuscript. Khalfan Abdulla was responsible for the conceptualization, methodology, literature search, thematic synthesis, and drafting of the manuscript. Rafiduraida Adulrahman supervised the study, contributed to the critical revision of the manuscript, and guided the research design. Both authors read and approved the final version prior to submission.
-

References

- Alamri, S., Kamuli, S., & Abdussamad, J. (2025). Optimizing human resources competence in the era of digital transformation as a strategic framework for crime prevention and handling. *Jurnal Inovasi Ilmu Sosial Dan Politik (JISoP)*, 7(2). <https://doi.org/10.33474/jisop.v7i2.24480>
- Alhajeri, M. (2022). *Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI)*. University of Salford (United Kingdom).
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, 98. <https://doi.org/10.1016/j.cose.2020.102003>
- Alzarooni, A. I., Alhashmi, S. M., Lataifeh, M., & Rice, J. (2024). Navigating digital transformation in the UAE: Benefits, challenges, and future directions in the public sector. *Computers*, 13(11), 281. <https://doi.org/10.3390/computers13110281>
- Elnaghi, M., Alshawi, S. N., Kamal, M. M., Weerakkody, V., & Irani, Z. (2019). Exploring the role of a government authority in managing transformation in service re-engineering – Experiences from Dubai police. *Government Information Quarterly*. <https://doi.org/10.1016/j.giq.2018.11.011>
- Fannur, F. (2025). Innovative Leadership Approaches for Enhancing Digital Governance and Collaborative Networks in Public Administration. *Journal Social Civilecial*, 1(2). <https://doi.org/10.71435/610487>
- Fest, I., Schäfer, M., van Dijck, J., & Meijer, A. (2023). Understanding data professionals in the police: a qualitative study of system-level bureaucrats. *Public Management Review*, 25(9). <https://doi.org/10.1080/14719037.2023.2222734>
- Gritt, E., Forsgren, E., & Pandza, K. (2024). Liminal digital transformation in public sector: The case of UK policing. *Journal of Strategic Information Systems*, 33(3). <https://doi.org/10.1016/j.jsis.2024.101851>
- Guenduez, A. A., Demircioglu, M. A., Mueller, E. M., & Cinar, E. (2025). Digital innovation strategies in the public sector. *Research Policy*, 54(8). <https://doi.org/10.1016/j.respol.2025.105274>
- Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly: Management Information Systems*, 23(1). <https://doi.org/10.2307/249410>
- Listianto, T. (2025). The Strategic Role of IT Capability in Police Organizational Transformation: Toward Smart Policing. *Indonesian Journal of Islamic Economics and Finance*, 5(2), 559–574. <https://doi.org/10.37680/ijief.v5i2.9386>
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Bmj*, 339.
- Thakur, A., Bhageerathy, R., Mithra, P., Sekaran, V. C., & Kumar, S. (2025). Navigating Organizational Challenges of Digital Transformation: A Qualitative Study of Meso-Level Public Health Officers in an Indian High-Priority Aspirational District. *Administrative Sciences*, 15(10). <https://doi.org/10.3390/admsci15100397>
- Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8. <https://doi.org/10.1186/1471-2288-8-45>
- Ushaka Adie, B., Tate, M., & Valentine, E. (2024). Digital leadership in the public sector: a scoping review and outlook. *International Review of Public Administration*, 29(1). <https://doi.org/10.1080/12294659.2024.2323847>

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*. <https://doi.org/10.1016/j.jsis.2019.01.003>