INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT SCIENCES
(ISSN: 2693-3500)
VOL.06 ISSUE05 (2026)

AMERICAN ACADEMIC PUBLISHER

Research Article

Organisational Models of External Stakeholder Engagement in the Implementation of Monitoring Systems

Ksenia Zagorskaya
Founder and CEO, XINFO TECH, Boston, MA, USA

check for updates

Received: 07 March 2026
Revised: 20 March 2026
Accepted: 17 April 2026
Published: 28 May 2026

Doi: 10.55640/ijbms-06-05-01

Page No: 01-10

Abstract

Monitoring systems in asset-intensive organisations depend on more than sensors, dashboards, and technical integration. Construction fleet telematics, smart-city platforms, and IoT-based operational systems require consent, coordination, and review from external stakeholders who control data access, public permissions, vendor interfaces, and compliance rules. Despite the rapid growth of the fleet telematics market — projected to expand from approximately USD 20 billion in 2025 to nearly USD 47 billion by 2034 — the organisational literature has not produced a structured model linking external stakeholder engagement to the specific decision sequence that monitoring-system projects follow. This review addresses that gap. It uses source analysis, comparative review, typologization, and conceptual synthesis to examine eighteen recent publications on public-sector digital transformation, smart-city data governance, construction digitalisation, collaborative governance, fleet telematics, stakeholder engagement frameworks, and data-privacy regulation. The review identifies three engagement models — centralised authorisation, distributed operational coordination, and hybrid governance — and proposes a five-gate implementation sequence connecting stakeholder classification, pilot perimeter design, data governance, operational escalation, and scale-up review. The article contributes a management-oriented implementation logic for large companies and public-facing operations where bureaucratic approval, city authority involvement, vendor dependency, and regulatory compliance shape the practical value of monitoring systems.

Keywords:

stakeholder engagement, monitoring systems, fleet telematics, data governance, digital implementation, hybrid governance, GDPR, decision rights.

INTRODUCTION

Monitoring systems in asset-intensive organisations depend on more than sensors, dashboards, and technical integration. Construction fleet telematics, smart-city platforms, and IoT-based operational systems require consent, coordination, and review from external stakeholders who control data access, public permissions, vendor interfaces, and compliance rules. A monitoring platform does not enter an organisation as a neutral technical object. Managers, vendors, compliance officers, and public actors must decide who authorises data collection, who validates alerts, and who acts when the system flags a delay or risk.

The market context makes this organisational gap increasingly consequential. The global fleet telematics market was estimated at approximately USD 20 billion in 2025 and is projected to grow at a compound annual rate of approximately 10 percent through 2034, driven by IoT integration, regulatory compliance demands, and the expansion of asset-intensive operations in construction, logistics, and public services [M1]. Despite this growth, technology adoption consistently faces non-technical barriers: integration complexity affects approximately 42 percent of deployments, data security concerns affect 46 percent, and

driver resistance affects 39 percent of organisations attempting implementation [M1]. These figures indicate that the primary constraint on monitoring-system adoption is not technical capability but organisational and governance readiness — precisely the dimension that the existing literature addresses in fragments rather than as a coherent model.

The organisational literature on digital transformation has developed substantial evidence about public-sector adoption, collaborative governance, and technology barriers. However, this literature rarely connects stakeholder engagement theory to the specific decision sequence that a monitoring-system project follows from piloting to scale-up. Researchers studying fleet telematics focus on technical architecture [4], while researchers studying smart-city governance focus on data rights and interoperability [5; 10] and researchers studying public-sector innovation focus on collaboration patterns [7; 9]. No existing study integrates these three bodies of evidence into a governance model specifically designed for the implementation of asset-monitoring and fleet-telemetry systems. This is the gap the present article addresses.

The novelty of this contribution rests on three dimensions. First, it operates at an intersection that is currently under-served: monitoring systems sit between operational technology (telematics, sensors, geofencing) and organisational governance (data rights, public permissions, vendor contracts), yet neither the operations-management literature nor the digital-governance literature has produced a framework that spans both sides. Second, the typology of three engagement models is derived from a cross-domain synthesis — drawing simultaneously on public-sector transformation research, smart-city governance, construction digitalisation, fleet telematics, implementation science, and data-privacy regulation — rather than from any single disciplinary tradition. Third, the five-gate implementation sequence translates the conceptual models into a practical decision instrument that practitioners can apply without specialist governance expertise. The article thus responds to a recognised need in the practitioner community: organisations deploying monitoring systems routinely encounter approval delays, data-rights disputes, and vendor-dependency problems that no existing framework addresses in an integrated way.

The central proposition is as follows: hybrid stakeholder governance — combining formal external authorisation of pilot boundaries with delegated operational adjustment — provides a stronger basis for monitoring-system implementation than either centralised authorisation or distributed coordination alone. This proposition is examined through comparative synthesis of the evidence base.

2. MATERIALS AND METHODS

2.1. Materials

The review corpus was assembled through purposive searches in Scopus, Web of Science, and Google Scholar using the following terms: stakeholder engagement; monitoring systems; digital governance; fleet telematics; smart-city data governance; public-sector digital transformation; hybrid governance; implementation frameworks; data privacy IoT; and construction digitalisation. Searches were restricted to publications from 2023 to 2026. Inclusion criteria required that a source address at least one of the following: stakeholder roles in digital implementation; governance of data-producing systems; barriers to construction or public-sector digitalisation; collaborative models for IoT-based services; or implementation-phase engagement structures. Purely technical studies without organisational relevance and broad digitalisation papers without stakeholder, governance, or implementation content were excluded.

The final corpus comprises eighteen sources: peer-reviewed articles, one OECD policy report, and two regulatory instruments. These cover seven research lines: public-sector transformation success and failure [1; 6]; digital innovation strategies in public organisations [2]; construction-sector digital barriers and fleet telematics [3; 4; 15]; smart-city data governance and IoT architecture [5; 10; 16]; collaborative governance and stakeholder demand [7; 7a; 9]; implementation-stakeholder engagement frameworks [8; 11; 14; 17; 18]; and data-privacy regulation as applied to IoT monitoring systems [13; 14].

2.2. Methods

The study uses comparative analysis to distinguish engagement models, source analysis to extract governance-related findings, typologization to classify stakeholder functions, conceptual synthesis to connect fleet monitoring with smart-city and public-sector literature, and analytical generalisation to build a management-oriented implementation model. Because the study is a conceptual review rather than an empirical test, the three engagement models and the five-gate implementation sequence presented in the Results and Discussion sections are propositions supported by the synthesised literature, not hypotheses verified through primary data collection. Empirical validation through comparative case studies across different regulatory and sector contexts is identified as a priority direction for future research.

3. RESULTS

Recent research on public-sector digital transformation provides a useful starting point for monitoring-system implementation. A systematic review of digital transformation success in the public sector identified 38 cases, four process types, and 51 success factors [1]. This evidence matters for monitoring systems because implementation depends on process design. Managers, vendors, compliance officers, and public actors must decide who authorises data collection, who validates alerts, and who acts when the system flags a delay or risk.

Research on digital innovation strategies in public organisations sharpens the same point. A study of 25 cities in 18 countries identified four strategy types: enhancement-oriented, anticipatory, adaptive, and persistent digital innovation [2]. Enhancement-oriented and persistent strategies were found to be the most prevalent, reflecting a strong focus on internal value creation through process optimisation and long-term organisational change, while adaptive and anticipatory strategies were comparatively less common [2]. Monitoring systems in construction fleets or urban operations follow a similar tension. Internal managers often justify the system through route throughput, equipment utilisation, or fuel control. External stakeholders assess the same system through public accountability, legal defensibility, privacy, interoperability, and urban impact. The project team must therefore translate operational efficiency into a language that city authorities, regulators, and senior committees can evaluate.

A critical explanation for why this translation fails lies in how different stakeholders frame the digital transformation process. A study of a council-wide digital transformation initiative in an Australian city council found that stakeholders hold fundamentally different interpretive frames — about the purpose of the system, the problems it is meant to solve, and who bears responsibility for its outcomes — and that successful implementation required deliberate frame alignment mechanisms rather than simple information-sharing [17]. In monitoring-system projects, this framing divergence is structural: vendors frame the system as a data product; operations teams frame it as a workflow tool; city authorities frame it as a public accountability instrument; and legal units frame it as a compliance risk. General consultation sessions expose these frames without resolving them. The engagement model must create structured moments at which each framing is brought to bear on a specific decision, with a named owner and a defined output.

The construction-sector literature shows that translation cannot rely solely on technical arguments. A study of barriers to digital transformation in circular construction identified contractors, investors, clients, waste managers, and government as influential stakeholders. The same study associated adoption barriers with skills, organisational culture, regulations, and stakeholder perceptions [3]. More recent research on digital transformation in construction organisations identified five primary barriers: high expenses, inappropriate organisational systems, operational inertia, training and skills difficulties, and stereotyped industry culture [15]. The concept of operational inertia is particularly relevant: once a dashboard enters daily use, adjustment becomes organisationally costly regardless of whether the underlying governance problems have been resolved. The implication is that data-rights, permission, and escalation decisions must be made before the system becomes operationally embedded, not after.

Fleet telematics research links these organisational questions to field operations. A 2026 study on an intelligent fleet monitoring system for earthwork equipment proposed a GNSS-based approach to real-time productivity management using configurable work areas, loading and dumping geofences, and web-based visualisation [4]. Field validation on active earthwork projects demonstrated classification and productivity estimation accuracy within 2.5 percent, while also highlighting that existing telematics frameworks depend on multiple sensing modules, which increases complexity and reduces flexibility for deployment under varying field conditions [4]. This finding supports treating vendors separately in stakeholder engagement models, because the choice of sensing architecture and platform determines which data fields the operator receives, how often updates arrive, and which integrations the analytics team can build.

Smart-city data governance literature extends the argument from operations to public legitimacy. The OECD report on smart-city data governance describes the pressure on cities from the growing number of actors involved in data production, analysis, sharing, and storage [5]. It identifies obstacles such as fragmented regulation, unclear stakeholder roles, limited local data capacity, interoperability problems, data security risks, and weak trust in public data stewardship [5]. These conditions closely resemble the external approval environment for monitoring systems that operate in public roads, construction zones, infrastructure assets, or municipal service areas.

The interoperability dimension is structural rather than incidental. Research on API-enabled interoperability in smart city systems distinguishes a data perspective — covering data standards, interoperability protocols, risk assessment, security, and governance — from a stakeholders' perspective — covering policies, regulations, data ownership, access, and privacy and trust [16]. This distinction maps directly onto the article's layer architecture: network and integration decisions belong to the data perspective and involve vendors and IT security; governance and regulatory decisions belong to the stakeholder perspective

and involve legal units, data protection officers, and municipal authorities. Collapsing both perspectives into a single vendor-facing integration conversation — a common implementation mistake — leaves public-legitimacy questions unresolved until they appear as compliance objections during scale-up.

Research on public-sector transformation failure provides the negative case. A study of a Sri Lankan government agency identified 23 failure factors grouped into organisational, implementing-agency, cultural, leadership, and macro-level themes [6]. This finding derives from a single revelatory case study in a developing-country context, and the specific failure mechanisms may not transfer directly to large corporate fleet or smart-city deployments in high-income settings. The general lesson — that implementation risk sits in the coordination gap between technical readiness and decision authority — retains broad relevance. A dashboard may function, yet field supervisors may distrust alerts, senior management may refuse to rely on the metrics, and external authorities may require additional documentation before the project scales.

Smart-city collaboration research offers a broader engagement model. A 2025 article on stakeholder collaboration and open innovation in smart cities developed a Quattro Helix model involving public administration, academia, business, and civil society [7]. The model highlights staged cooperation, stakeholder roles, implementation guidelines, and performance indicators. Monitoring-system projects need its sequencing logic: external engagement should begin at problem definition, continue through pilot design, and return during review. The same research group has since proposed a Sixfold Helix model that adds the natural environment and a digital technology and infrastructure sector as distinct actors [7a]. This extension is directly relevant to IoT-based monitoring because it gives vendors and data-infrastructure providers an explicit structural role, rather than treating them as a subset of the business helix.

The human-machine-organisation view adds a theoretical bridge between digital infrastructure and managerial behaviour. A 2024 article on digital governance developed an integrative perspective on humans, machines, and organisations in public management [8]. Monitoring systems create this triangle in practical terms. Sensors and algorithms classify operational states. Dispatchers and supervisors interpret the classifications. Organisations decide which classifications count as evidence for intervention, review, or escalation. External stakeholders then test the legitimacy of these decisions. A municipal authority may accept GPS-based monitoring as an operational tool while rejecting uncontrolled secondary use of location records.

Empirical evidence from Swiss municipalities shows that external actors can accelerate collaboration. A survey of 720 municipalities found that stakeholder demand and digital change agents strongly influenced digitalisation-related collaboration, while internal resources alone did not explain collaboration with the same strength [9]. External pressure becomes useful when managers convert it into a structured authorisation path with named owners, deadlines, and review criteria.

IoT-based smart-city architecture provides a clear way to organise stakeholder engagement along the data path. A 2024 review describes smart-city systems through perception, network, and application layers [10]. In monitoring-system projects, these layers correspond to different stakeholder questions. The perception layer raises questions for field operators, site owners, and public-space actors. The network layer raises questions for vendors, IT security teams, and procurement teams. The application layer raises questions for operations managers, senior leadership, and compliance teams. Figure 1 adapts this architectural logic to stakeholder engagement, adding a governance layer and a feedback layer to address the public and regulatory dimensions that the standard three-layer model does not cover.

Research on stakeholder engagement in implementation science offers a complementary framework. The Implementation-STakeholder Engagement Model (I-STEM), developed in the context of large-scale health-IT implementation, argues that stakeholder engagement must be structured as a set of discrete activities across implementation phases rather than as general consultation [11]. Different stages — piloting, field adjustment, and scale-up — require different actors and different types of decision authority, and collapsing them into a single engagement event regularly produces unresolved objections at later stages. Research on stakeholder engagement-as-practice in public sector innovation confirms this finding from a different disciplinary tradition: content analysis of OECD Observatory of Public Sector Innovation case studies found that engagement practices need to be adapted to the specific tasks of each implementation phase rather than applied uniformly across the project lifecycle [18].

Digital governance of infrastructure projects provides further evidence that structured decision assignment outperforms broad participation. Research on decision-making and stakeholder engagement in infrastructure projects found that IoT can improve transparency and accountability, but only when governance arrangements clearly assign which stakeholders hold which decision rights at which project stage [12]. Without that assignment, digital tools generate data without generating actionable decisions.

Data-privacy regulation introduces a further dimension that the organisational models must accommodate. Monitoring systems that collect location data, personnel movement, or sensor records in European jurisdictions operate under the General Data Protection Regulation (GDPR). GDPR requirements for lawful basis, purpose limitation, data minimisation, storage limits, and

subject rights determine what data the system may collect, how long it may retain records, who may access them, and under what conditions secondary analysis is permitted [13]. For fleet monitoring that tracks driver location and behaviour during working hours, GDPR requires operators to document a lawful basis for processing — typically the performance of a contract or the pursuit of legitimate interests — and to ensure that drivers are informed of what data is captured and why [14]. Where monitoring is classified as high-risk processing, a data protection impact assessment (DPIA) is mandatory before the system goes live. Equivalent frameworks apply in other jurisdictions. In practice, this means that data governance cannot be treated as an internal administrative task: it requires documented engagement with legal units, data protection officers, and — where monitoring touches employees or public-space subjects — with representatives of those subjects.

[Figure 1 — Stakeholder Engagement Map]

Physical operation and monitored asset Monitored asset and field operation form the starting point of the data flow.
Perception layer Process: Sensors, GPS/GNSS, telemetry, geofences Stakeholders: Field operators, site managers, equipment owners
Network and integration layer Process: API, vendor platform, cloud transfer, interoperability Stakeholders: Vendors, IT security, procurement, data owners
Application layer Process: Dashboards, alerts, efficiency ratios, reporting Stakeholders: Operations managers, headquarters, supervisors
Governance layer Process: Permissions, data rights (incl. GDPR / applicable regulatory framework), public-sector alignment, audit trail Stakeholders: Regulators, municipal authorities, legal units, data protection officers, senior management
Feedback layer Process: Pilot review, norm revision, escalation rules, scaling decision Stakeholders: Cross-functional steering group and external reviewers

Figure 1. *Stakeholder Engagement Map for Monitoring-System Implementation, adapted from [10], with governance and feedback layers added.*

The reviewed sources identify three organisational models of stakeholder engagement. The centralised authorisation model concentrates decision-making power in senior management, legal units, municipal representatives, or a formal steering committee. This model suits regulated or politically sensitive settings because it leaves a visible approval record. Its weakness appears during field learning: operational teams may wait for approval before adjusting dashboards, threshold labels, or escalation routines.

The distributed operational coordination model gives greater initiative to operations teams, field supervisors, vendors, and analysts. It supports faster testing because people close to the monitored process can correct dashboard logic and field procedures. Its weakness appears when a pilot touches public space, regulated assets, or vendor-controlled data. External actors may receive information too late, and the organisation may lose time rebuilding trust or documentation.

The hybrid governance model separates formal boundaries from operational adjustment. External stakeholders approve the

pilot perimeter, data-use rules, escalation limits, and review schedule. Operational teams work inside those boundaries and adjust configuration, response rules, and reporting formats during testing. This model draws support from several sources simultaneously: public-sector success-factor research highlights process conditions [1]; construction digitalisation research identifies stakeholder-specific barriers [3; 15]; fleet telematics research shows the operational constraints of platform-dependent data [4]; smart-city governance research stresses data rights and coordination [5; 16]; implementation-stakeholder engagement research demonstrates the value of stage-specific engagement structures [11; 18]; and municipal collaboration research shows the practical force of external demand [9].

The comparison suggests a final result: stakeholder groups differ by the uncertainty they control. Municipal authorities control permission uncertainty. Vendors control integration uncertainty. Regulators and legal units control compliance uncertainty, including the specific requirements of applicable data-protection law. Headquarters controls resource uncertainty. Field supervisors and dispatchers control usability uncertainty. Monitoring-system projects lose time when teams discuss these uncertainties in separate conversations. Projects gain implementation discipline when managers sequence them as connected decision gates.

4. DISCUSSION

A monitoring-system project requires an engagement model that treats external stakeholders as holders of specific decision rights. General consultation produces weak results because it rarely clarifies who can block data collection, who can approve a pilot, who can change an alert rule, and who can authorise scale-up. The implementation team needs a compact governance design with named stakeholders and defined decisions.

The first step is to classify stakeholders by decision function. Municipal authorities and regulators are part of the permission group. Vendors and IT security teams belong to the data-transfer and integration group. Senior management belongs to the resource and approval group. Field supervisors, dispatchers, and site managers are part of the usability group. Legal and compliance units — including data protection officers where required by applicable regulation — are part of the data-rights group. This classification prevents a common implementation mistake: inviting many actors into one discussion while leaving the actual decision unresolved. Research on stakeholder engagement-as-practice confirms that the most effective public sector innovation projects are those where engagement is differentiated by phase and decision type rather than delivered as a uniform consultation exercise [18].

The framing divergence identified by Hoblos, Sandeep and Pan [17] provides a further reason why classification by decision function matters. When different stakeholders hold incompatible interpretive frames — vendors framing the system as a data product, legal units framing it as a compliance risk, city authorities framing it as a public-accountability instrument — placing all of them in the same conversation without assigning specific decisions to specific actors produces lengthy discussion without resolution. The engagement model must create structured moments at which each framing is brought to bear on a bounded decision, not an open agenda.

The second step is pilot perimeter design. The organisation defines monitored assets, data fields, geographic zones, dashboard users, escalation rules, and external reporting boundaries. In construction fleet operations, this perimeter may cover GPS/GNSS traces, dwell time, idle time, fuel records, zone labels, and colour-coded efficiency categories. The perimeter document should remain short enough for decision makers to read. It should name the monitored process, list what the pilot will not use the data for, and identify which data fields are subject to regulatory constraints. Where GDPR or an equivalent framework applies, the perimeter document should specify the lawful basis for each data type and identify whether any fields trigger high-risk processing obligations.

The third step is data governance before operational dependence begins. The project team defines access rights, storage periods, vendor responsibilities, audit logs, anonymisation where required, and restrictions on secondary use. These rules must be established in alignment with applicable law. Where GDPR applies, a data protection impact assessment is required for high-risk monitoring activities, particularly those involving systematic tracking of individuals in public spaces or employment contexts [13; 14]. If managers postpone these rules until after the dashboard enters daily use, every later revision will disrupt operations and invite compliance review. The operational inertia documented in the construction-sector literature [15] means that the cost of revision rises sharply once the system is embedded in daily workflows.

The fourth step is bounded operational learning. External stakeholders approve the perimeter and review schedule. Dispatchers, supervisors, analysts, and vendors adjust alert wording, dashboard layout, and response routines within that boundary. This arrangement keeps formal approval intact while giving the operational team enough room to correct the system during field use.

Table 1 compares the three engagement models. It helps select a governance form by regulatory exposure, vendor dependency, and the required speed of field learning.

Table 1. Comparison of Stakeholder Engagement Models for Monitoring-System Implementation

Model	Decision centre	External stakeholder function	Main strength	Main risk	Suitable setting
Centralised authorisation	Senior management, legal units, municipal or regulatory representatives	Formal permission, compliance review, data-use approval	Clear accountability and approval trace	Slow adjustment during field testing	Public-facing pilots, regulated assets, politically sensitive sites
Distributed operational coordination	Operations team, field supervisors, vendors, analytics unit	Technical support, local coordination, informal feedback	Fast correction of dashboard logic and workflows	Weak formal acceptance and late external objections	Internal pilots with limited public exposure
Hybrid governance	Steering group with delegated operational team	Boundary approval, data governance (incl. regulatory compliance), periodic review, escalation control	Formal legitimacy with room for field learning	Coordination burden and need for clear decision rules	Large companies, mixed public-private settings, vendor-dependent telematics projects

The model separates permission, integration, field use, and review. City authorities do not need to approve each dashboard edit. Dispatchers do not need to negotiate data retention rules during daily work. Vendors do not define public acceptability. Each group receives a limited decision zone.

A practical implementation sequence should contain five gates. Gate 1 classifies stakeholders and their decision rights. Gate 2 fixes data governance and vendor integration rules, including regulatory compliance requirements and any required DPIA. Gate 3 secures pilot authorisation from senior management and external authorities where required. Gate 4 governs field use through escalation logs and response procedures. Gate 5 reviews pilot evidence and decides whether to scale, revise, or close the project.

Table 2 turns this sequence into a decision logic. The purpose is to keep the project from moving to technical deployment while external approval, data rights, or response authority remain vague.

Table 2. Decision Logic for External Stakeholder Engagement During Monitoring-System Implementation

Stage	Decision question	Required stakeholder input	Practical output	Escalation trigger
Stakeholder classification	Which actors control permission, data, integration, resources, or field use?	Operations, legal, IT security, vendor, and public authority where relevant	Stakeholder decision map	Missing owner for approval, data access, or field response
Pilot perimeter	Which assets, zones, data fields, and decisions fall inside the pilot?	Headquarters, operations, compliance, and external authority	Pilot perimeter note (incl. regulatory constraints on each	Demand to expand monitored territory or add sensitive data fields

		where relevant	data field)	
Data governance (incl. regulatory compliance)	Who may collect, store, share, audit, and reuse monitoring data? What legal framework applies?	Legal, IT security, vendor, data owner, DPO, regulator where relevant	Data-use protocol, access matrix, DPIA where required	Unclear ownership, weak audit trail, vendor restriction, regulatory non-compliance
Operational use	Which alerts require action, and who records the response?	Dispatchers, supervisors, analytics unit, vendor support	Escalation rules and response log	Repeated false alerts, delayed response, and field resistance
Review and scale-up	Which evidence justifies continuation, revision, or closure?	Steering group, operations, and external reviewers where required	Scale-up decision or revision plan	Compliance dispute, weak adoption, unresolved vendor dependency

The decision logic provides the implementation team with a concrete way to manage bureaucratic approvals. It reduces ambiguity before daily operations depend on the monitoring system. The greatest risk in these projects is premature stabilisation: a dashboard becomes routine before the organisation settles access rights, public permissions, and escalation authority. Once supervisors use a dashboard for daily decisions, later changes become harder to justify and harder to govern — a dynamic consistent with the operational inertia finding in the construction-sector literature [15].

Monitoring metrics should cover two fields. The first field measures system performance: data completeness, update delays, alert accuracy, response time, unresolved red-status events, dashboard use, and number of manual overrides. The second field measures stakeholder engagement: approval lead time, unresolved objections, vendor response time, data-access exceptions, number of escalated pilot changes, and completion of scheduled review meetings. These metrics help managers see whether the project fails because the system performs poorly or because the engagement structure blocks practical use.

The proposed model has boundaries. It fits monitoring systems with identifiable data flows, vendor dependency, and external stakeholder exposure. A small internal dashboard with no public authority involvement, no regulated asset, and no sensitive location data may not require this level of governance. The model also depends on delegated authority: if senior management approves a pilot but refuses to let the operations team adjust working rules within the approved boundary, hybrid governance becomes centralised authorisation with additional meetings. The regulatory dimension varies by jurisdiction and sector, and the five-gate sequence should be calibrated to the applicable legal framework.

For construction fleet monitoring, the model gives a workable publication-level contribution. It uses the domain logic of telemetry, geofencing, efficiency bands, vendor APIs, and dispatch response without claiming access to confidential company data or reporting unpublished performance results. The article's value lies in the organisational model: who approves, who integrates, who acts, who audits, and who decides whether the pilot deserves scale-up.

5. CONCLUSION

The implementation of a monitoring system depends on the distribution of decision rights among external stakeholders. Municipal authorities, vendors, regulators, headquarters, legal units, data protection officers, and field actors control different uncertainties. The review confirms that implementation gains stability when managers map these uncertainties before pilot deployment.

Centralised authorisation gives projects formal legitimacy but slows field learning. Distributed operational coordination accelerates practical testing but leaves open approval and data-governance risks. Hybrid governance offers the most coherent model for bureaucratic and public-facing environments because it combines formal pilot boundaries with delegated operational adjustment.

The proposed implementation logic connects stakeholder classification, pilot perimeter, data governance including regulatory compliance, operational escalation, and scale-up review. This sequence supports monitoring systems in construction fleets, urban operations, and infrastructure-related settings where external approval, vendor-controlled data, and applicable data-

protection law shape adoption.

The contribution of this article is threefold. Conceptually, it synthesises evidence from five disciplinary traditions — public management, construction digitalisation, smart-city governance, implementation science, and data-privacy regulation — into a single governance framework for monitoring-system implementation. Typologically, it classifies three engagement models and defines their decision centres, stakeholder functions, strengths, risks, and suitable settings. Practically, it proposes a five-gate implementation sequence and a two-field metric structure that implementation teams can apply without specialist governance expertise. The conceptual synthesis supports the proposition that hybrid stakeholder governance provides a stronger basis for monitoring-system implementation than centralised authorisation or distributed coordination alone. Empirical validation of this proposition through comparative case studies across regulatory and sector contexts represents the primary direction for future research.

REFERENCES

1. Escobar, F., Almeida, W. H. C., & Varajão, J. (2023). Digital transformation success in the public sector: A systematic literature review of cases, processes, and success factors. Information Polity, 28(1), 61–81. DOI: 10.3233/IP-211518.

2. Guenduez, A. A., Demircioglu, M. A., Mueller, E. M., & Cinar, E. (2025). Digital innovation strategies in the public sector. Research Policy, 54(8), 105274. DOI: 10.1016/j.respol.2025.105274.

3. Hassan, A. M., Negash, Y. T., & Hanum, F. (2024). An assessment of barriers to digital transformation in circular construction: An application of stakeholder theory. Ain Shams Engineering Journal, 15(7), 102787. DOI: 10.1016/j.asej.2024.102787.

4. Lee, S., Sharafat, A., Yoo, S.-H., & Seo, J. (2026). Intelligent fleet monitoring system for productivity management of earthwork equipment. Applied Sciences, 16(2), 1115. DOI: 10.3390/app16021115.

5. OECD. (2023). Smart city data governance: Challenges and the way forward. OECD Urban Studies. OECD Publishing. DOI: 10.1787/e57ce301-en.

6. Syed, R., Bandara, W., & Eden, R. (2023). Public sector digital transformation barriers: A developing country experience. Information Polity, 28(1), 5–27. DOI: 10.3233/IP-220017.

7. Tutak, M., & Brodny, J. (2025). Stakeholder collaboration and open innovation in smart cities: A Quattro Helix model for technological and social transformation. Journal of Open Innovation: Technology, Market, and Complexity, 11(3), 100594. DOI: 10.1016/j.joitmc.2025.100594.

7a. Brodny, J., & Tutak, M. (2025). Towards a sixfold helix model for green smart cities? A conceptual exploration of stakeholder collaboration, interaction mechanisms, and role allocation. Journal of Open Innovation: Technology, Market, and Complexity, 11(4), 100681. DOI: 10.1016/j.joitmc.2025.100681.

8. Vigoda-Gadot, E., & Mizrahi, S. (2024). The digital governance puzzle: Towards integrative theory of humans, machines, and organizations in public management. Technology in Society, 77, 102530. DOI: 10.1016/j.techsoc.2024.102530.

9. Weißmüller, K. S., Ritz, A., & Yerramsetti, S. (2023). Collaborating and co-creating the digital transformation: Empirical evidence on the crucial role of stakeholder demand from Swiss municipalities. Public Policy and Administration. Advance online publication. DOI: 10.1177/09520767231170100.

10. Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A review of IoT-based smart city development and management. Smart Cities, 7(3), 1462–1501. DOI: 10.3390/smartcities7030061.

11. Potthoff, S., Finch, T., Bührmann, L., Etzelmüller, A., van Genugten, C. R., Girling, M., May, C. R., Perkins, N., Vis, C., Rapley, T., & on behalf of the ImpleMentAll consortium. (2023). Towards an Implementation-STakeholder Engagement Model (I-STEM) for improving health and social care services. Health Expectations, 26(5). DOI: 10.1111/hex.13808.

12. Tumpa, R. J., & Naeni, L. (2025). Improving decision-making and stakeholder engagement at project governance using digital technology for sustainable infrastructure projects. Smart and Sustainable Built Environment, 14(4), 1292–1329. DOI: 10.1108/SASBE-10-2024-0451.

13. European Parliament and Council. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Official Journal of the European Union, L 119, 1–88.

14. Information Commissioner's Office. (2023). Employment practices and data protection: Monitoring workers. ICO Guidance. Available at: https://ico.org.uk.

15. Halder, S. (2025). Digital transformation in the construction industry: Barriers and leadership competencies. In D. Bajaj (Ed.), Handbook of Construction Project Management. Springer, Singapore. DOI: 10.1007/978-981-96-7631-6_25.

16. Anthony Jnr, B. et al. (2024). Enabling seamless interoperability of digital systems in smart cities using API: A systematic literature review. Journal of Urban Technology. DOI: 10.1080/10630732.2024.2427543.

17. Hoblos, N., Sandeep, M. S., & Pan, S. L. (2024). Achieving stakeholder alignment in digital transformation: A frame transformation perspective. Journal of Information Technology, 39(4), 630–649. DOI: 10.1177/02683962231219518.

18. Knox, S., Marin-Cadavid, C., & Oziri, V. (2025). Stakeholder engagement-as-practice in public sector innovation. International Public Management Journal, 28(1), 153–168. DOI: 10.1080/10967494.2024.2423952.

Market Data Reference

1. M1. Market Research Future. (2025). Fleet Telematics Market Analysis: Size, Share and Forecast 2025–2034. MRFR Report ID MRFR/AM/38293-HCR. Available at: https://www.marketresearchfuture.com/reports/fleet-telematics-market-40320. [Accessed May 2026].