International Journal of Pedagogics

VOLUME Vol.05 Issue12 2025
PAGE NO. 226-230
DOI 10.37547/ijp/Volume05Issue12-62

Challenges Encountered When Transitioning To Digital Management

Karimova Mahbuba Muzaffarovna

2nd-year Master's student at Puchon University, Deputy Director at State Preschool Education Institution No. 89., Uzbekistan

Received: 20 October 2025; **Accepted:** 11 November 2025; **Published:** 17 December 2025

Abstract: Transitioning to digital management is often framed as a technology refresh, but in practice it is a sociotechnical transformation that alters decision rights, operational controls, accountability models, and the organization's risk posture. Even when modern platforms are procured and deployed successfully, many organizations fail to realize expected gains in speed, transparency, and performance because constraints originate in governance, legacy architecture, data quality, capability gaps, and external dependencies rather than in software features. This article analyzes the most persistent challenges encountered during transitions to digital management and explains how these challenges reinforce one another through feedback effects such as fragmented ownership, "tool-first" implementation, and transformation fatigue. The discussion focuses on governance and strategic alignment, legacy systems and technical debt, data governance maturity, workforce skills and cultural adoption, cybersecurity and privacy requirements, third-party dependency and resilience expectations, and measurement difficulties that obscure value realization. The article concludes that successful digital management is less about digitizing existing routines and more about redesigning management as an operating model grounded in trusted data, explicit decision rights, and resilient digital operations.

Keywords: Digital management, digital transformation, change management, legacy systems, data governance, cybersecurity, operational resilience, third-party risk.

Introduction: Digital management can be defined as the systematic organization of managerial work—planning, coordination, monitoring, decision-making, and control—through integrated digital platforms and data-driven workflows. In mature forms, it includes unified process orchestration across functions, standardized data definitions, real-time or near-real-time reporting, and governance mechanisms that keep data, automation, and access controls consistent with the organization's policies and regulatory obligations. The transition to digital management is therefore not limited to introducing software; it reshapes how authority is exercised, how performance is measured, and how operational risk is managed.

Organizations pursue digital management for understandable reasons. Leadership expects shorter decision cycles, lower coordination costs, better transparency, reduced human error, stronger auditability, and improved ability to scale services without proportional increases in headcount. Digital tools can also enable new operating capabilities such as predictive analytics, automated control testing, and continuous monitoring. However, digital management transitions often stall after early wins. Dashboards may exist without trust, workflows may be digitized without eliminating handoffs, and new platforms may coexist with legacy systems in ways that multiply complexity rather than reducing it.

A core reason is that management is a control system. When an organization shifts from manual coordination to platform-mediated coordination, the controls move into data structures, entitlements, workflow rules, and integration logic. If governance is weak, the digital system mirrors fragmented authority; if data governance is immature, reporting becomes contested; if capabilities are uneven, adoption becomes partial; if resilience is insufficient, operations become more brittle under stress. These dynamics explain why digital management is frequently experienced as "more tools, more complexity," even when the technology itself is modern.

This article examines the key challenges that consistently appear in digital management transitions and synthesizes them into an integrated interpretation. The objective is to clarify why these obstacles persist, how they interact, and what their presence implies for organizations seeking to manage the transition responsibly and effectively.

This article uses a structured narrative synthesis approach. The analysis draws on established literature on digital transformation and change management, research and practitioner perspectives on legacy modernization and technical debt, systematic insights on data governance implementation, and contemporary frameworks addressing cybersecurity governance and operational resilience. The objective is not to provide a tool-specific evaluation, but to identify cross-sector challenge patterns that remain stable across different technologies and industries.

The synthesis is organized using a sociotechnical lens. Under this lens, digital management is treated as an operating model that must align five domains: governance and decision rights; people and skills; processes and controls; data and technology architecture; and risk, security, and resilience. Challenges are interpreted as interdependent because digital management failures rarely result from a single cause. Instead, a weakness in one domain typically amplifies weaknesses in others, creating cumulative friction and undermining confidence in the transformation.

The most decisive challenge in digital management transitions is governance: who owns the transformation, who makes decisions when priorities conflict, and how tradeoffs are resolved between speed, standardization, cost, and risk. Many organizations begin digital initiatives with broad aspirations—becoming "data-driven," "paperless," or "agile"—but without converting these aspirations into managerial outcomes that can guide design decisions. When goals remain abstract, implementation tends to drift toward what vendors demonstrate well or what individual departments request, producing a platform landscape that is technically functional yet operationally incoherent.

Digital management intensifies this problem because the platform encodes governance. Access controls, workflow approvals, data definitions, and exception rules are not neutral configurations; they represent a management philosophy. If governance is not settled early, the platform becomes an arena in which organizational power dynamics are replayed. Departments resist standardization if it reduces local discretion, while central functions resist customization if it undermines comparability. Without clear decision rights, the organization accumulates compromises that satisfy no one: processes are digitized but retain manual checkpoints, data is integrated but definitions remain inconsistent, and reporting exists but requires "reconciliation narratives" that erode trust.

Effective governance also must integrate technology risk as a management concern. In digitally managed operations, failures in identity, access control, logging, or incident handling become failures of management itself. A governance approach that treats cybersecurity as an IT responsibility rather than an enterprise responsibility commonly leads to late-stage remediation, delays, and unresolved risk acceptance decisions. Over time, such patterns convert digital management from a performance initiative into an ongoing negotiation between delivery urgency and risk containment.

Legacy systems are not merely old technologies; they are repositories of business rules, historical exceptions, and organizational memory. They often sit at the center of core operations and are entangled with a network of interfaces, spreadsheets, and informal workarounds that evolved over years. Digital management transitions confront legacy constraints in two ways. First, legacy platforms may not support real-time data access or standardized integration patterns, limiting the feasibility of unified workflows. Second, legacy-driven processes often embed manual controls that were designed to compensate for unreliable data, slow interfaces, and limited visibility. Digitizing such processes without redesigning them can preserve the very frictions the organization seeks to eliminate.

A common response is partial modernization: organizations layer new portals, workflow tools, or analytics platforms on top of existing systems. This can produce rapid improvements in user experience and reporting appearance, but it tends to increase integration complexity. Each new layer introduces additional synchronization points and new failure modes. Technical debt grows because the organization now maintains both the old system and the new integration scaffolding. When issues occur, root-cause analysis becomes harder because data lineage spans multiple platforms, and operational teams may not understand where truth resides.

Partial modernization can still be strategically valid when it is governed as a staged architecture roadmap rather than an accumulation of tactical patches. The difficulty is that staged modernization requires strong enterprise architecture discipline, consistent funding over multiple years, and stability in leadership priorities. In environments where budgets are annual and leadership changes frequently, partial modernization becomes permanent. Digital management then inherits the limitations of legacy systems while adding complexity in the name of modernization.

Digital management is only as effective as the data it uses to represent reality. Yet many organizations enter transformation with inconsistent data ownership, fragmented master data, and limited enforcement mechanisms. Data governance is often described in policy terms—data owners, data stewards, definitions—but the operational challenge is ensuring that governance becomes executable: that definitions are implemented across systems, that quality thresholds are monitored, that lineage is documented, and that change control is enforced when new data sources are added.

The trust deficit emerges quickly. If managers observe that dashboards contradict operational experience, they revert to informal sources. If operational staff see that entering data accurately increases workload but provides little local benefit, they input minimal information or create parallel tracking files. If data corrections are frequent and opaque, finance, risk, and operations disagree about performance, and the platform becomes a contested space rather than a shared reference point. Once trust declines, adoption becomes superficial: users comply with required steps but avoid relying on the system for decisions, undermining the intent of digital management.

Data governance maturity is particularly challenging when organizations attempt to implement advanced analytics or AI before stabilizing foundational data. Advanced models amplify data problems because they are sensitive to inconsistencies and because their outputs can appear authoritative even when based on incomplete or biased inputs. Organizations therefore experience a paradox: the more sophisticated the analytics toolset, the more the organization depends on disciplined data governance, yet the culture and structures for governance are often least developed at the moment when analytic ambitions are highest.

Digital management requires new skills and new professional identities. Managers must interpret data, understand process logic, and make decisions that are traceable and consistent with governance rules. Operational staff must adapt to standardized workflows and new accountability mechanisms that come with logged actions and automated controls. Technical and product teams must maintain platforms as evolving products rather than as completed projects. Where these capabilities are insufficient, the transition is experienced as a burden rather than an enablement.

Cultural resistance is frequently a rational response to poorly designed change. If a digital management system is introduced without process simplification, it can increase time spent on compliance steps and data entry. If training focuses on clicking through screens rather than on the logic of the new operating model, users may follow procedures mechanically without understanding their purpose, making errors more likely and exception handling slower. If the system is perceived as surveillance rather than as support, adoption declines and informal workarounds increase.

Transformation fatigue also emerges as a material risk. Digital management transitions rarely occur in a vacuum; they overlap with reorganizations, cost programs, new compliance requirements, and shifting strategic priorities. When employees experience continuous change without clear stabilization periods, cognitive overload grows. The organization may then lose experienced staff precisely when process knowledge and mentoring are most needed. This loss deepens dependency on external consultants and vendors, which can further reduce internal ownership and long-term sustainability.

As management becomes digital, the organization’s operational integrity becomes dependent on cybersecurity and privacy controls. Digital management platforms consolidate sensitive operational and personal data, centralize access, and create new pathways for misuse. Security incidents can therefore degrade not only confidentiality but also the credibility of the management system. If employees fear that systems are insecure or that data is used in unintended ways, their willingness to record accurate information declines. If customers or partners lose confidence in the organization’s data handling, the organization faces reputational and regulatory consequences.

Cybersecurity challenges are intensified during transitions because transformation periods expand complexity. New integrations are built rapidly, identity systems are modified, and external services are onboarded. Each change introduces misconfiguration risk. If cybersecurity governance is not embedded into transformation governance, security becomes a late-stage gate that delays releases, encourages bypass behavior, or results in exceptions that accumulate into unacceptable residual risk.

Privacy considerations require equal attention. Digital management systems often enable more granular monitoring of work patterns, communications, and productivity indicators. Even if such monitoring is intended for legitimate performance improvement, it can generate mistrust if it is not transparent, proportionate, and governed. Trust is a managerial asset; without it, digitized management becomes contested and adoption becomes defensive.

Digital management increasingly relies on third parties. Cloud platforms host critical applications; vendors provide workflow engines, analytics tools, identity services, and collaboration systems; managed service providers operate infrastructure and security monitoring. These dependencies can increase agility and reduce costs, but they also reshape the organization's risk boundary. Management outcomes become dependent on external service reliability, vendor patch cycles, contractual obligations, and concentration risk.

Operational resilience expectations have risen accordingly, particularly in regulated sectors. Organizations are increasingly expected to define critical operations, understand dependencies, and demonstrate their ability to continue delivering key services through disruptions. In digital management contexts, resilience is not a separate program; it is embedded in architecture decisions, vendor selection, backup and recovery design, and incident response readiness. Where resilience is treated as an afterthought, digital management can paradoxically reduce operational continuity by making the organization more dependent on a small number of platforms without sufficient contingency planning.

Third-party dependency also complicates accountability. When service degradation occurs, internal teams may struggle to diagnose issues because telemetry and root-cause data reside with vendors. This can slow recovery, increase operational downtime, and produce disputes about responsibility. Mature digital management transitions therefore require disciplined vendor governance, clear service-level expectations, and operational procedures for dependency failures.

Digital management produces more metrics, but more metrics do not automatically produce better management. During transitions, metrics can be misleading because data definitions evolve, adoption is uneven, and processes are unstable. Leaders may see conflicting signals: productivity appears down because time is spent learning new tools, compliance appears worse because problems that were previously hidden are now visible, and customer outcomes fluctuate due to transition disruptions. In such conditions, organizations can misinterpret early indicators and make harmful decisions, such as cutting transformation resources too early or shifting scope repeatedly, creating churn.

Value realization also suffers when organizations confuse outputs with outcomes. Deploying a platform, digitizing a form, or launching a dashboard is an output. Improved decision speed, fewer errors, better customer experience, and stronger compliance are outcomes. If governance does not define outcome metrics clearly and link them to process redesign and accountability, the organization may declare success prematurely while underlying management practices remain unchanged.

A frequent end-state of poor measurement is "visibility without action." Dashboards show problems, but ownership of remediation is unclear; workflows generate alerts, but teams are overloaded; analytics identifies risks, but decision-making remains politically constrained. Digital management then becomes informational rather than transformational. The platform is present, but managerial behavior is unchanged, and therefore performance does not improve proportionately.

The transition to digital management is a transformation of the organization's management system, not a software installation. The most persistent challenges arise from governance weaknesses, legacy constraints, data governance immaturity, capability gaps, cultural and trust dynamics, heightened cybersecurity and privacy requirements, expanding third-party dependencies, and measurement problems that obscure value realization. These challenges reinforce one another, producing predictable failure patterns such as fragmented implementation, partial adoption, and increasing operational complexity.

Organizations that succeed typically treat digital management as an operating model design problem. They clarify decision rights and accountability early, stage legacy modernization with architectural discipline, invest in data governance as an executable capability, build workforce skills as a strategic asset, embed cybersecurity governance into enterprise governance, manage third-party dependencies as part of operational continuity, and define outcome-based metrics that connect digital visibility to managerial action. When these elements align, digital management can deliver its intended benefits: faster decisions, more reliable operations, improved transparency, and stronger resilience.

REFERENCES

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: NIST, 2024.
2. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0: Resource & Overview Guide. NIST SP 1299. Gaithersburg: NIST, 2024.

3. OECD. 2023 OECD Digital Government Index. Paris: OECD Publishing, 2024.
4. OECD. Developing Skills for Digital Government. Paris: OECD Publishing, 2024.
5. Omol E.J. Organizational digital transformation: from evolution to future trends // Digital Transformation and Society. 2024. Vol. 3, No. 3.
6. Shonubi O.A. Innovation challenges of digital transformation // Digital Business. 2025.
7. Bernardo B.M.V. Data governance & quality management—Innovation and maturity assessment models: systematic review // Data & Knowledge Engineering. 2024.
8. Bassi C.A., et al. Challenges to implementing effective data governance // Proceedings of an International Conference on Information Systems and Data Governance. 2023.
9. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Brussels, 2022.
10. Commission Delegated Regulation (EU) 2024/1532 (Regulatory technical standards under Regulation (EU) 2022/2554). Brussels, 2024.
11. Reuters. Amazon and Google named by EU among “critical” tech providers for the finance industry. 18 November 2025.
12. Saeed S. Editorial: Digital transformation and cybersecurity challenges // Frontiers in Computer Science. 2025.
13. McKinsey & Company. Unlocking success in digital transformations. Analytical report. 2018.
14. ITPro. Heavy workloads and botched digital initiatives are causing “transformation fatigue”. 2025.
15. Zangana H.M. From Legacy Systems to Digital Solutions: Change Management in IT Transformations. 2025.