

ORIGINAL RESEARCH

Open access

Digital Vendor Portfolio Management: A Framework for Coordinating SaaS Providers, Payment Platforms, Analytics Tools, and Outsourced Digital Services

Sara Ben Youssef^{1*}, Amal Trabelsi¹

Abstract

Modern businesses increasingly depend on a wide array of digital vendors, including SaaS applications, payment gateways, analytics platforms, and outsourced digital services. These vendors no longer sit at the periphery of operations; they shape how firms sell, serve, analyse, automate, and innovate. As digital transformation deepens, the vendor landscape becomes more complex, distributed, and strategically consequential. Many firms still manage digital vendors through fragmented ownership structures, with procurement, IT, finance, marketing, operations, and business units each controlling different vendor relationships. This siloed approach produces integration debt, uncontrolled spending, duplicated functionality, weak renewal discipline, and fragmented data flows. It also increases dependency on external platforms and service providers whose pricing, APIs, data policies, and continuity risks can directly affect firm performance. The objective of this article is to develop a Digital Vendor Portfolio Framework that enables firms to coordinate and govern all digital vendors as an integrated strategic portfolio. The framework treats digital vendors not as isolated contracts but as interdependent assets, risks, and capabilities. It provides a governance logic for mapping vendor roles, identifying dependencies, monitoring performance, and aligning external digital resources with business strategy. The proposed framework addresses coordination for SaaS providers, payment platforms, analytics tools, and outsourced digital services. It identifies governance mechanisms for each vendor category and outlines how portfolio mapping, contractual safeguards, technical integration, relational governance, and performance dashboards can reduce complexity. The article argues that proactive digital vendor portfolio management is now a strategic imperative for firms seeking efficiency, data integrity, resilience, and control.

Keywords Digital vendor portfolio, SaaS coordination, Payment platforms, Analytics tools, Outsourced digital services, Vendor governance

*Correspondence:

Sara Ben Youssef
sara.benyoussef@utunis.tn

¹ Department of Digital Enterprise Studies, Faculty of Economics and Management, University of Tunis, Tunis, Tunisia

Introduction

Digital business has shifted enterprise technology from a bounded internal infrastructure to a dispersed network of external applications, platforms, and service providers.

Digital innovation research shows that organisations increasingly create value through recombining digital resources and externally connected innovation systems, making vendor ecosystems central to strategic execution

[1]. As platforms and infrastructures become embedded in everyday operations, the boundary between internal capability and external vendor dependence becomes increasingly difficult to govern [2].

The result is a proliferation of digital vendors that often accumulates faster than formal governance can adapt. Cloud applications, analytics tools, automation services, marketing platforms, payment gateways, and outsourced

development partners may each be justified locally, yet collectively they create vendor sprawl, overlapping functionality, and fragmented accountability. Research on IT consumerisation and shadow IT shows that business units frequently adopt technologies outside traditional IT control, creating governance challenges that are both technical and organisational [3].

This fragmentation produces several forms of hidden debt. Integration debt emerges when SaaS applications and platforms are connected through fragile interfaces, manual exports, or ad hoc middleware, while data fragmentation undermines analytics quality and organisational learning. Big data and analytics research emphasises that value depends not only on access to tools but also on governance, capability development, and the ability to turn distributed data resources into coordinated decisions [4].

The aim of this article is to propose a Digital Vendor Portfolio Framework that gives firms an integrated governance logic for managing digital vendors as a strategic asset class. Existing work on digital transformation stresses that firms must realign structures, capabilities, and governance mechanisms as digital technologies reshape business models [5]. Building on that insight, this article argues that vendor management must move beyond contract administration toward continuous portfolio coordination, dependency monitoring, and strategic alignment.

Digital Vendor Portfolio Management

Digital vendor portfolio management can be defined as the coordinated governance of a firm's full set of external digital providers across applications, platforms, data services, infrastructure, and outsourced digital capabilities. This function is distinct from traditional IT procurement because it focuses not only on acquisition cost but also on interoperability, risk concentration, innovation contribution, and strategic fit. The platform literature suggests that digital value increasingly emerges through ecosystems of complementary actors, making portfolio-level orchestration more important than bilateral supplier control alone [6].

A portfolio perspective also recognises that digital vendors differ in strategic importance and substitutability. Some vendors provide commodity functionality and can be replaced with limited disruption, while others become

deeply embedded in customer journeys, payment flows, decision systems, or core operational processes. Research on platform ecosystems as meta-organisations highlights how dependence on external platforms can reshape power, control, and coordination across organisational boundaries [7].

Digital vendor portfolio management therefore requires continuous evaluation rather than episodic sourcing. Firms must assess vendor performance, contractual flexibility, data portability, integration quality, security exposure, and alignment with evolving business priorities. Studies of organisational agility show that IT capabilities contribute to performance when firms can reconfigure digital resources quickly and coherently rather than merely accumulate technologies [8].

The framework developed in this article addresses four major vendor categories: SaaS providers, payment platforms, analytics tools, and outsourced digital services. These categories reflect different governance problems, but they are interconnected through data flows, customer processes, APIs, contracts, and shared operational dependencies. Digital transformation research indicates that organisations need dynamic capabilities to repeatedly sense, seize, and reconfigure digital resources, which makes the coordinated management of external vendors a continuing strategic responsibility [9].

SaaS Provider Coordination

SaaS providers have become the most visible expression of digital vendor proliferation because they are easy to acquire, rapidly deployable, and often purchased directly by business units. This accessibility supports experimentation and responsiveness, but it also increases the likelihood of subscription sprawl, duplicated tools, inconsistent data definitions, and weak lifecycle governance. Shadow IT research shows that decentralised technology adoption can create innovation benefits while also weakening enterprise oversight when governance mechanisms fail to adapt [10].

The central coordination problem in SaaS portfolios is not simply the number of tools but the interdependence among them. Customer relationship management, marketing automation, collaboration, finance, human resources, and analytics systems often exchange data through APIs, connectors, or manual workflows that evolve without a coherent architecture. Research on cloud provider

management indicates that firms need structured processes for provider selection, monitoring, relationship management, and exit planning when cloud services become operationally significant [11].

SaaS coordination also requires governance of renewal cycles, user access, data ownership, service levels, security compliance, and integration standards. A SaaS application may appear inexpensive when evaluated as an isolated subscription, yet its real cost includes integration maintenance, training, data cleansing, workflow redesign, and switching barriers. Studies of cloud computing and the changing role of IT suggest that internal IT functions remain essential because they coordinate external services, manage architectural coherence, and preserve organisational control [12].

Effective SaaS portfolio governance combines central visibility with distributed business ownership. Firms need a shared inventory of applications, common criteria for approval and renewal, standardised integration requirements, and dashboards that connect vendor performance to business outcomes. **Table 1** summarises the challenges and coordination mechanisms for managing a portfolio of SaaS providers.

Table 1. SaaS Provider Coordination: Challenges, Integration Requirements, and Governance Mechanisms

SaaS portfolio challenge	Integration requirement	Governance mechanism	Strategic contribution
Subscription sprawl across business units	Central inventory of active tools, owners, users, renewal dates, and costs	Portfolio register with approval, renewal, and retirement rules	Reduce duplication and improve spending discipline
Fragmented customer, employee, or operational data	Standard APIs, data models, synchronisation rules, and master-data ownership	Enterprise integration standards and data stewardship roles	Improve data consistency and decision quality
Shadow IT adoption outside formal IT oversight	Lightweight intake process for business-led SaaS requests	Joint governance between IT, procurement, finance, and	Preserve local agility while restoring control

		business units	enterprise visibility
Weak contract and renewal control	Renewal calendar, usage analytics, exit terms, and data retrieval clauses	Contract playbooks and renewal review boards	Strengthen negotiating power and avoid automata lock-in
Security and compliance inconsistencies	Identity management, access controls, audit logs, and security certifications	Vendor risk tiering and periodic compliance reviews	Protect sensitive data and reduce operational exposure
Integration debt from ad hoc connectors	Architecture review before deployment and change management for integrations	Technical design authority and integration health monitoring	Maintain architectural coherence as the SaaS stack evolves

Payment Platform and Analytics Tool Dependence

Payment platforms and analytics tools create a distinctive form of digital vendor dependence because they sit close to revenue capture, customer data, and managerial decision-making. Payment gateways, digital wallets, fraud-screening providers, and embedded finance interfaces influence transaction continuity, fee exposure, customer experience, and settlement visibility. FinTech research shows that financial-service innovation increasingly depends on platformised infrastructures, which can create both efficiency gains and new dependencies on external intermediaries [13].

The governance challenge is especially acute because payment vendors combine technical integration with commercial and regulatory consequences. A change in fee structure, risk policy, authentication process, API availability, or settlement timing can quickly affect margins and customer conversion. Digital platform ecosystem research suggests that firms operating through platform arrangements must manage not only direct service quality

but also dependence on the rules, interfaces, and control choices of platform owners [14].

Analytics tools introduce a parallel but data-centred dependency. Dashboards, attribution systems, customer analytics platforms, and business intelligence tools shape what managers see, measure, and optimise, yet these systems often depend on externally controlled algorithms, proprietary data schemas, and opaque pricing tiers. Research on analytics value creation shows that firms gain performance benefits only when analytics tools are embedded within organisational capabilities, decision routines, and data governance practices rather than treated as standalone technologies [15].

The combined dependence on payment and analytics vendors exposes firms to lock-in, data access constraints, continuity risks, and measurement bias. Firms should therefore evaluate these vendors by their contribution to resilience, data portability, transparency, and strategic flexibility, not only by functionality or cost. **Table 2** outlines the dependencies and governance gaps associated with payment platforms and analytics tools.

Table 2. Payment Platform and Analytics Tool Dependence: Strategic Vulnerabilities, Data Control Issues, and Mitigation Strategies

Vendor category	Strategic vulnerability	Data control issue	Governance gap
Payment gateways	Transaction disruption, fee escalation, settlement delays, and authentication failures	Limited visibility into fraud scoring, settlement logic, and transaction-level metadata	Vendor assessed mainly on processing cost rather than operational resilience
Digital wallets and embedded payment platforms	Dependence on external customer interfaces and platform rules	Restricted access to customer transaction behaviour and wallet-level analytics	Weak negotiation power when customer adoption concentrates on one platform

Fraud and risk-screening services	False positives, declined transactions, and customer-experience damage	Opaque algorithms and limited explainability of risk decisions	Insufficient review of algorithmic performance and appeal mechanisms
Web and product analytics tools	Measurement bias, tracking disruption, and attribution instability	Proprietary metrics, sampling limits, and constrained historical export	Tool adoption without enterprise data definitions or stewardship
Customer data and marketing analytics platforms	Lock-in through identity graphs, segmentation models, and automation rules	Vendor-controlled data enrichment, model outputs, and audience portability	Overreliance on vendor dashboards for strategic decisions
Business intelligence and visualisation tools	Proliferation of inconsistent dashboards and duplicated reporting logic	Fragmented semantic layers and competing definitions of key metrics	Decentralised report ownership without governance of data meaning

Outsourced Digital Service Control

Outsourced digital services extend the vendor portfolio beyond platforms and applications into externally performed work such as software development, customer support, digital marketing, automation, data engineering, and AI/ML services. These relationships differ from SaaS subscriptions because the vendor is not merely providing a tool but actively shaping artefacts, customer interactions, code quality, campaign execution, and operational knowledge. Research on IT outsourcing in digital transformation shows that outsourcing relationships increasingly move from transactional delivery toward

Outsourced digital service control also requires cultural alignment and knowledge retention. Firms that outsource too much digital expertise risk losing the internal capability needed to evaluate vendor claims, specify requirements, and protect strategic knowledge. **Table 3** identifies control mechanisms and performance monitoring practices for outsourced digital services.

Table 3. Outsourced Digital Service Control: Contractual, Relational, and Technical Governance of External Digital Service Providers

Outsourced digital service	Contractual governance	Relational governance	Technical governance
Software development	Clear scope, IP ownership, code escrow where appropriate, security	Joint sprint reviews, product-owner involvement, and shared	Code repositories controlled by the client, architectural standards

	obligations, and acceptance criteria	backlog prioritisation	automated testing, and secure development rules
Digital marketing	Campaign scope, data-use limits, brand guidelines, attribution rules, and termination rights	Regular learning reviews, creative feedback loops, and transparent performance discussions	Access controls for accounts, tagging standards, and consent-compliant tracking
Customer support outsourcing	Service levels, escalation rules, data-protection clauses, and customer-experience standards	Calibration sessions, shared scripts, and feedback loops with internal teams	Secure access to support platforms, audit logs, and knowledge base governance
AI/ML and analytics services	Model ownership, training-data rights, confidentiality, explainability expectations, and audit rights	Cross-functional model review, ethical-risk discussion, and domain-expert participation	Version control, model monitoring, bias testing, and data lineage documentation
Automation and process services	Responsibility for bot failures, continuity obligations, and change-control provisions	Joint process redesign workshops and incident retrospectives	Process documentation, access controls, monitoring logs, and fallback procedure
Digital design and experience services	Deliverable ownership, accessibility standards, brand	Co-creation workshops, user-feedback reviews, and	Design-system repositories, prototype traceability

	consistency, and usability expectations	design- system alignment	and analyti integration
--	---	--------------------------------	----------------------------

Proposed Digital Vendor Portfolio Framework

The Digital Vendor Portfolio Framework begins with the premise that vendors must be evaluated as an interdependent portfolio rather than as isolated contracts. Each vendor is mapped according to strategic importance, operational criticality, substitutability, data sensitivity, integration depth, and switching cost. Research on digital innovation and transformation indicates that firms need governance structures capable of coordinating external digital resources while preserving strategic flexibility and innovation capacity [19].

The first layer of the framework is portfolio mapping. SaaS applications, payment platforms, analytics tools, and outsourced service providers are placed into categories such as strategic partners, operational utilities, specialised capabilities, experimental tools, and retirement candidates. This mapping logic reflects strategic information systems research showing that agility depends on the firm's ability to identify which digital resources should be scaled, integrated, replaced, or reconfigured [20].

The second layer is governance architecture, which combines contractual, relational, and technical controls. Contractual governance specifies rights, obligations, pricing, service levels, data access, exit terms, and intellectual property; relational governance supports trust, adaptation, escalation, and shared learning; technical governance manages APIs, identity, security, data flows, and architectural standards. Research on board IT governance emphasises that oversight mechanisms are most effective when they complement organisational capabilities rather than operate as symbolic controls [21].

The third layer is coordination rhythm, which turns the framework into a repeatable management system. Quarterly portfolio reviews, renewal boards, integration health checks, vendor risk tiering, and performance dashboards allow firms to detect sprawl, dependency, underperformance, and emerging strategic opportunities. **Table 4** presents the proposed Digital Vendor Portfolio Framework integrating all vendor categories.

Table 4. Digital Vendor Portfolio Framework: Portfolio Mapping, Governance Layers, and Coordination across SaaS, Payment, Analytics, and Outsourced Services

Framework component	SaaS providers	Payment platforms	Analytics tools
Portfolio mapping	Map applications by business owner, function, users, data sensitivity, renewal date, and integration depth	Map providers by transaction volume, geography, fees, continuity role, and customer-experience impact	Map tools to data source, metric ownership, decision use, model opacity, and exportability
Strategic classification	Classify as core workflow system, departmental tool, experimental tool, or retirement candidate	Classify as primary processor, backup provider, specialised payment method, or high-risk dependency	Classify as enterprise decision platform, tactical reporting tool, modelling service, or redundant dashboard
Contractual governance	Renewal discipline, data return rights, security obligations, audit clauses, and usage-based pricing review	Fee controls, service continuity clauses, settlement obligations, data access rights, and exit planning	Raw-data export, metadata transparency, model documentation, privacy compliance, and pricing safeguards
Relational governance	Joint planning with business owners and vendor success teams	Escalation routines with payment partners and operational-risk owners	Analytics governance forums linking technical and business use

Technical governance	API standards, identity management, integration monitoring, and master-data alignment	Redundancy design, transaction monitoring, authentication controls, and incident testing	Data lineage metric governance access controls, and validation against source systems
Coordination rhythm	SaaS renewal reviews and application rationalisation cycles	Payment resilience reviews and fee benchmarking	Dashboard rationalisation and analytics quality review

Figure 1 illustrates how the Digital Vendor Portfolio Framework converts fragmented digital vendor relationships into an integrated governance system linking portfolio visibility, vendor-category coordination, governance layers, and strategic outcomes.

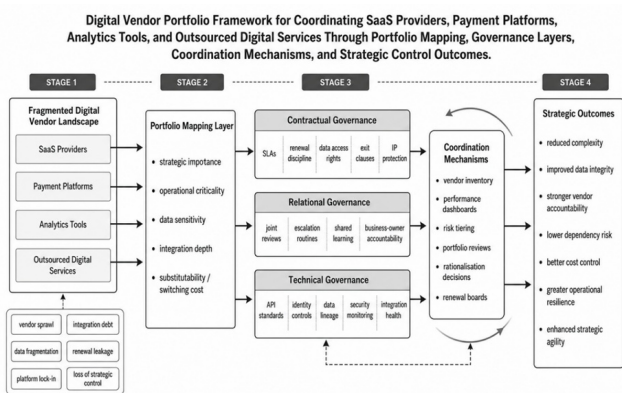


Figure 1. Digital Vendor Portfolio Framework for Coordinating SaaS Providers, Payment Platforms, Analytics Tools, and Outsourced Digital Services Through Portfolio Mapping, Governance Layers, Coordination Mechanisms, and Strategic Control Outcomes

Implementation Strategy

Implementation should begin with a complete vendor inventory that captures contracts, owners, users, costs, renewal dates, data categories, integrations, service levels, and business processes supported by each vendor. This

inventory should be followed by categorisation according to strategic importance, substitutability, risk level, and integration depth. Research on digital transformation stresses that firms need a coordinated view of technologies, organisational change, and strategy before they can govern digital resources effectively [22].

The second step is to establish a governance structure that brings together IT, procurement, finance, legal, security, data governance, and business-unit leaders. This structure should create decision rights for new vendor approval, renewal review, rationalisation, exception handling, and escalation. Research on digital transformation as strategy and organisational change shows that governance must be embedded across organisational roles rather than isolated in a single technical function [23].

The third step is to integrate vendor performance data into regular portfolio reviews. Dashboards should combine spend, usage, service quality, integration health, security posture, business value, and dependency risk so that management can see the portfolio as a living system. Analytics capability research shows that performance gains depend on dynamic capabilities and the ability to transform data resources into coordinated action, which makes the vendor dashboard both a monitoring device and a learning mechanism [24].

Managerial Implications

The first managerial implication is that digital vendor portfolio management should be elevated to a senior strategic concern. As firms become dependent on external digital providers for payments, analytics, customer engagement, operations, and innovation, vendor decisions affect resilience, margins, compliance, and competitive differentiation. Research on big data analytics and firm performance indicates that technology value depends on managerial capability and organisational alignment, not merely on tool adoption [25].

The second implication is that firms should invest in integration and governance tools rather than relying on spreadsheets, informal knowledge, or contract archives. A portfolio view requires visibility into data flows, access rights, APIs, vendor performance, renewal timing, and functional overlap across the enterprise. Research on robotic process automation illustrates how externally enabled digital tools can reshape workflows, but also how

governance is needed to avoid fragile automation and poorly controlled process change [26].

The third implication is that managers must build internal capabilities even when they outsource digital work. Firms need enough architectural, analytical, commercial, and legal expertise to evaluate vendor claims, negotiate safeguards, monitor performance, and retain strategic knowledge. Strategic information systems research shows that innovation capacity and organisational agility depend on internal competence as well as external resources, so outsourcing cannot substitute for informed governance [27–29].

Conclusion

A siloed approach to digital vendors is no longer viable. SaaS applications, payment platforms, analytics tools, and outsourced digital services now form an interdependent operating environment that shapes efficiency, data integrity, customer experience, and strategic control. When these relationships are governed separately, firms risk accumulating hidden complexity, duplicated spending, integration debt, and dependency on external actors they do not fully understand.

The Digital Vendor Portfolio Framework developed in this article offers a practical tool for integrated vendor governance. It helps firms map vendor roles, classify strategic importance, align governance intensity with risk, coordinate contractual and technical controls, and institutionalise recurring portfolio reviews. Its central contribution is to shift digital vendor management from local

contract administration to enterprise-level portfolio stewardship.

Future research should empirically validate the framework across industries, firm sizes, and digital maturity levels. Researchers could examine how portfolio governance affects cost control, resilience, innovation speed, data quality, and bargaining power in digital ecosystems. For managers, the immediate priority is to adopt a portfolio mindset and treat the digital vendor landscape as a strategic system that must be deliberately designed, monitored, and renewed.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 10 Dec 2025 Revised: 25 Jan 2026 Accepted: 10 Mar 2026
Published online: 18 March 2026

Rights and permissions

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

Nambisan S, Lyytinen K, Majchrzak A, Song M. Digital innovation management: Reinventing innovation management research in a digital world. *MIS Q.* 2017;41(1):223–38.

Constantinides P, Henfridsson O, Parker GG. Introduction—platforms and infrastructures in the digital age. *Inf Syst Res.* 2018;29(2):381–400.

Gregory RW, Kaganer E, Henfridsson O, Ruch TJ. It Consumerization and the transformation of it governance1.

MIS Q. 2018;42(4):1225-53.

Günther WA, Mehrizi MH, Huysman M, Feldberg F. Debating big data: A literature review on realizing value from big data. *J Strateg Inf Syst.* 2017;26(3):191-209.

Vial G. Understanding digital transformation: A review and a research agenda. *Managing digital transformation*. Cham: Springer; 2021. p. 13–66.

De Reuver M, Sørensen C, Basole RC. The digital platform: A research agenda. *J Inf Technol.* 2018;33(2):124-35.

Kretschmer T, Leiponen A, Schilling M, Vasudeva G. Platform ecosystems as meta-organizations: Implications for platform strategies. *Strateg Manag J.* 2022;43(3):405-24.

Queiroz M, Tallon PP, Sharma R, Coltman T. The role of IT application orchestration capability in improving agility and performance. *J Strateg Inf Syst.* 2018;27(1):4-21.

Warner KS, Wäger M. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Plann.* 2019;52(3):326-49.

Haag S, Eckhardt A. Shadow it. *Bus Inf Syst Eng.* 2017;59(6):469-73.
<https://doi.org/10.1007/s12599-017-0497-x>.

Oesterle S, Jöhnk J, Keller R, Urbach N, Yu X. A contingency lens on cloud provider management processes. *Bus Res.* 2020;13(3):1451-89.

Vithayathil J. Will cloud computing make the Information Technology (IT) department obsolete?. *Inf Syst J.* 2018;28(4):634-49.

Gomber P, Kauffman RJ, Parker C, Weber BW. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *J Manag Inf Syst.* 2018;35(1):220-65.

Hein A, Schrieck M, Riasanow T, Setzke DS, Wiesche M, Böhm M, et al. Digital platform ecosystems. *Electron Markets.* 2020;30(1):87-98.

Wamba SF, Gunasekaran A, Akter S, Ren SJ, Dubey R, Childe SJ. Big data analytics and firm performance: Effects of dynamic capabilities. *J Bus Res.* 2017;70:356-65.

Gratzke L, Zimmer MP, Drews P. IT outsourcing relationships in the context of digital transformation: From transactional relationships to ecosystem partnerships. *Inf Syst Manag.* 2026;43(1):65-84.

Oshri I, Dibbern J, Kotlarsky J, Krancher O. An information processing view on joint vendor performance in multi-sourcing: the role of the guardian. *J Manag Inf Syst.* 2019;36(4):1248-83.

Vidgen R, Shaw S, Grant DB. Management challenges in creating value from business analytics. *Eur J Oper Res.* 2017;261(2):626-39.

Kohli R, Melville NP. Digital innovation: A review and synthesis. *Inf Syst J.* 2019;29(1):200-23.

Tallon PP, Queiroz M, Coltman T, Sharma R. Information technology and the search for organizational agility: A systematic review with future research possibilities. *J Strateg Inf Syst.* 2019;28(2):218-37.

Turel O, Liu P, Bart C. Is board IT governance a silver bullet? A capability complementarity and shaping view. *Int J Acc Inf Syst.* 2019;33:32-46.

Verhoef PC, Broekhuizen T, Bart Y, Bhattacharya A, Dong JQ, Fabian N, et al. Digital transformation: A multidisciplinary reflection and research agenda. *J Bus Res.* 2021;122:889-901.

Hanelt A, Bohnsack R, Marz D, Antunes Marante C. A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *J Manag Stud.* 2021;58(5):1159-97.

Mikalef P, Boura M, Lekakos G, Krogstie J. Big data analytics capabilities and innovation: the mediating role of dynamic capabilities and moderating effect of the environment. *Br J Manag.* 2019;30(2):272-98.

Müller O, Fay M, Vom Brocke J. The effect of big data and analytics on firm performance: An econometric analysis considering industry characteristics. *J Manag Inf Syst.* 2018;35(2):488-509.

Hofmann P, Samp C, Urbach N. Robotic process automation. *Electron Markets.* 2020;30(1):99-106.

Ravichandran T. Exploring the relationships between IT competence, innovation capacity and organizational agility. *J Strateg Inf Syst.* 2018;27(1):22-42.

Yeow A, Soh C, Hansen R. Aligning with new digital strategy: A dynamic capabilities approach. *J Strateg Inf Syst.* 2018;27(1):43-58.

Grover V, Chiang RH, Liang TP, Zhang D. Creating strategic business value from big data analytics: A research framework. *J Manag Inf Syst.* 2018;35(2):388-423.