Vokatek: Journal of Research and Community Service
E-ISSN: 2986-0105 P-ISSN : 2985-8402
Vol. 4, No. 3, December 2026
https://journal.diginus.id/VOKATEK/index

Digital Transformation Capability and Accounting Information Resilience: Mediating AI-Driven Analytics and Moderating Cybersecurity Governance

Napiajo[1], *Marjono*[2], *Tia Apriani*[3], *Lia Nurina*[4], *Alexander Virgiawan Liany Oleona*[5]
[1,2,3] *Institut Bisnis dan Ekonomi Indonesia, Indonesia*
[4,5] *Politeknik Negeri Pontianak, Indonesia*

Corresponding e-mail : napiajo@gmail.com

ARTICLE INFO

Keywords:

Accounting Information Resilience;
AI-Driven Analytics Capability;
Cybersecurity Governance;
Digital Transformation Capability;
SMEs

Article History

Received: September 09, 2026
Revised: October 01. 2026
Accepted:October 19, 2026

ABSTRACT

Digital transformation is reshaping how micro, small, and medium-sized enterprises (MSMEs) generate, analyze, protect, and recover accounting information, yet the mechanisms through which digital capability may contribute to accounting information resilience remain insufficiently integrated. This study develops a capability-based framework linking Digital Transformation Capability (DTC) to Accounting Information Resilience (AIR) through AI-Driven Analytics Capability (AIAC), while positioning Cybersecurity Governance (CSG) as a boundary condition. The study is conceptual in orientation and employs an illustrative benchmark PLS-SEM specification based on a hypothetical structure of 300 digitally engaged MSMEs across six districts of Pontianak City, Indonesia. The benchmark specification is used solely to demonstrate the internal analytical logic of the proposed moderated-mediation model and should not be interpreted as empirical evidence. The illustrative pattern reflects the theoretical expectation that DTC may strengthen AIAC and AIR, that AIAC may serve as an intermediate capability through which digital transformation is translated into more resilient accounting-information processes, and that stronger CSG may enhance the effectiveness of this proposed mechanism. The study contributes by distinguishing accounting information resilience from conventional information quality, identifying AI-enabled analytics as a potential capability-conversion mechanism, and conceptualizing cybersecurity governance as a condition that may strengthen resilience outcomes. The framework provides a theoretically grounded and testable basis for future empirical validation using observed MSME data and for comparative research across emerging-market digital ecosystems.

This is an open access article under the CC BY-SA license

To cite this article : Napiajo, Marjono, Apriani, T., Nurina, L., & Oleona, A. V. L. (2026). Digital transformation capability and accounting information resilience: Mediating AI-driven analytics and moderating cybersecurity governance. *Vokatek: Journal of Research and Community Service, 4*(3), XX–XX. https://doi.org/10.61255/vokatek.v4i3.2022

INTRODUCTION

Digital transformation has evolved from a discretionary technology initiative into an organizational capability that reshapes how firms configure resources, redesign processes, and generate information for decision-making. This development is particularly important for micro, small, and medium-sized enterprises (MSMEs), which often operate under resource constraints, limited managerial slack, and strong dependence on a relatively small set of digital systems. Digital transformation should therefore not be understood merely as the adoption of software, cloud services, digital payments, or automated bookkeeping. Rather, it represents an organization-

wide process in which digital technologies trigger strategic responses, alter value-creation activities, and require corresponding changes in organizational structures, routines, and managerial practices (Vial, 2019). From a dynamic-capability perspective, its value depends on whether firms can sense digitally enabled opportunities and risks, seize them through coordinated action, and transform organizational routines as technological and environmental conditions change (Warner & Wäger, 2019).

This capability-based perspective helps explain why MSMEs with comparable levels of technology adoption may achieve different information and organizational outcomes. Digital transformation capability (DTC) reflects the ability to coordinate digital technologies, human competencies, organizational processes, and managerial routines rather than simply possessing digital assets. Sousa-Zomer et al. (2020) describe digital transforming capability as being rooted in complementary microfoundations, including digitally competent human resources, digital intensity, and an enabling organizational context. In accounting functions, such capability can improve transaction capture, reconciliation, reporting, monitoring, forecasting, and internal control. At the same time, increasing digitalization generates larger, faster, and more interconnected flows of accounting data. Consequently, digital transformation may contribute to more resilient accounting information directly by strengthening digitally enabled processes and indirectly by enabling firms to develop more advanced analytical capabilities.

One capability that may explain this indirect mechanism is AI-driven analytics capability (AIAC). Analytics creates organizational value when firms combine data, technological infrastructure, managerial knowledge, technical expertise, and routines for systematic interpretation rather than relying on technology investment alone (Gupta & George, 2016). When analytics incorporates artificial intelligence, machine learning, automated classification, anomaly detection, forecasting, and pattern recognition, firms can move beyond retrospective reporting toward more anticipatory and exception-oriented information processing. In accounting settings, AI-enabled analytics can support the detection of unusual transactions, cash-flow forecasting, reconciliation, identification of control signals, and faster managerial responses. AIAC is therefore conceptualized as the organizational ability to integrate and repeatedly use AI-enabled analytical resources to generate decision-relevant insights from operational and accounting data.

The distinction between AI adoption and AI capability is especially important for MSMEs. Most MSMEs are unlikely to develop proprietary AI infrastructures; instead, they access AI-enabled functionality through accounting applications, cloud platforms, payment systems, dashboards, inventory applications, enterprise software, and third-party services. Mikalef and Gupta (2021) conceptualize AI capability as a multidimensional organizational ability involving data, technology, human expertise, coordination, organizational change capacity, and risk orientation. Accordingly, the contribution of AI to accounting processes depends not simply on whether AI functionality is available, but on whether it is embedded in repeatable organizational routines. DTC can therefore provide the technological and organizational foundation from which AIAC develops, while AIAC can serve as the more proximate mechanism through which digital resources are converted into reliable, adaptive, and responsive accounting-information processes.

The focal outcome of this study is accounting information resilience (AIR), which is related to but distinct from conventional accounting information quality. Accounting information quality generally evaluates whether accounting outputs are accurate, relevant, complete, understandable, and timely under existing operating conditions. In contrast, resilience concerns the capacity of accounting-information processes to remain dependable or recover rapidly when disruptions occur. Drawing on research linking digital transformation with organizational resilience (He et al., 2022) and accounting information quality (Song et al., 2026), this study conceptualizes AIR as the capacity of accounting-information processes to preserve or rapidly restore integrity, availability, continuity, adaptability, and recoverability under conditions such as system failure, cyber incidents, abrupt operational change, or data disruption. This distinction is important because a system may generate high-quality accounting information during stable operations while remaining vulnerable when disruption makes information inaccessible, inconsistent, unverifiable, or difficult to recover.

Digitalization, however, creates a governance challenge. Greater connectivity, automation, system integration, and data concentration can improve analytical capability while simultaneously increasing exposure to unauthorized access, credential compromise, data manipulation, ransomware, service interruption, and other cyber-related risks. These risks may be particularly significant for MSMEs because digital dependence can develop more rapidly than formal governance structures. Cybersecurity governance (CSG) addresses this imbalance by defining security responsibilities, establishing policies and access controls, monitoring cyber risks, coordinating incident responses, and assigning recovery responsibilities. Hoong and Rezania (2024) demonstrate that cybersecurity in smaller firms is shaped not only by technical safeguards but also by organizational agency, strategic orientation, internal motivation, and external pressures. In accounting environments, this governance dimension is critical because analytical capability cannot consistently produce resilient information when the underlying data, system access, processing environment, and recovery arrangements are inadequately governed.

Accounting-related studies support the importance of cybersecurity but leave an important contingency unresolved. Nhan et al. (2025) show that accounting information security controls are influenced by technological conditions, policies and regulations, human resources, and organizational culture, while stronger controls contribute to internal-control effectiveness. Maldonado et al. (2026) further associate cybersecurity practices with accounting information-system quality and accounting information quality in the MSME context. However, these studies primarily treat cybersecurity as an antecedent of system, control, or information-quality outcomes. They do not establish whether cybersecurity governance changes the strength with which analytical capability is converted into resilient accounting information. This distinction matters because AIAC may improve anomaly detection, forecasting, and response speed, but these benefits are likely to be more effective when governance simultaneously protects data integrity, regulates system access, clarifies accountability, and supports incident response and recovery.

The resulting research gap concerns the integration of these capability and governance mechanisms. Existing studies have separately linked digital transformation with organizational resilience (He et al., 2022), digital transformation with accounting information quality (Song et al., 2026), AI capability with organizational

outcomes (Mikalef & Gupta, 2021), and cybersecurity practices with accounting controls and information-system quality (Nhan et al., 2025; Maldonado et al., 2026). What remains insufficiently explained is how digital transformation contributes specifically to the resilience of accounting information, through which organizational capability this relationship operates, and under what cybersecurity-governance conditions the conversion becomes stronger or weaker. This study addresses this gap by integrating DTC, AIAC, AIR, and CSG within a single moderated-mediation framework. In this framework, AIAC represents the mechanism through which DTC is translated into AIR, while CSG represents the boundary condition that may strengthen the effectiveness of this conversion.

Pontianak City, West Kalimantan, provides a relevant empirical setting for examining these relationships because rapid business digitalization coexists with continuing financial-management and capability-development needs. As of 15 June 2026, 49,569 Business Identification Numbers (*Nomor Induk Berusaha* or NIB) had been issued in Pontianak, with 98% associated with micro and small enterprises (Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Pontianak, 2026). Municipal records also reported 186,753 QRIS merchants in 2025, representing a 12.89% year-on-year increase (Pemerintah Kota Pontianak, 2026b). At the same time, local government programs continued to provide training in digital cash-flow management and digital financial reporting, indicating that bookkeeping and financial-management capabilities remain areas requiring development (Pemerintah Kota Pontianak, 2026a). These conditions provide a setting in which digital adoption is widespread enough to support variation in technology-enabled business processes, while differences in analytical capability, cybersecurity governance, and accounting-information resilience are still likely to remain meaningful.

Based on the preceding arguments, this study proposes the following hypotheses:

H1: Digital Transformation Capability has a positive effect on Accounting Information Resilience.

H2: Digital Transformation Capability has a positive effect on AI-Driven Analytics Capability.

H3: AI-Driven Analytics Capability has a positive effect on Accounting Information Resilience.

H4: AI-Driven Analytics Capability mediates the relationship between Digital Transformation Capability and Accounting Information Resilience.

H5 : Cybersecurity Governance positively moderates the relationship between AI-Driven Analytics Capability and Accounting Information Resilience, such that the relationship becomes stronger at higher levels of Cybersecurity Governance.

H6: Cybersecurity Governance positively moderates the indirect effect of Digital Transformation Capability on Accounting Information Resilience through AI-Driven Analytics Capability, such that the indirect effect becomes stronger at higher levels of Cybersecurity Governance.

Accordingly, this study examines how and under what cybersecurity-governance conditions DTC contributes to AIR through AIAC in digitally engaged MSMEs. The study makes three principal contributions. First, it extends dynamic-capability reasoning into the accounting-information domain by distinguishing AIR from conventional accounting information quality and emphasizing integrity, availability, continuity,

adaptability, and recoverability under disruption. Second, it identifies AIAC as the capability-based mechanism through which digital transformation can be translated into resilient accounting-information processes. Third, it positions CSG as a boundary condition that may determine whether AI-enabled analytical capabilities generate stronger resilience outcomes. By integrating capability formation, analytical mediation, and governance contingency within one model, the study advances beyond simple technology-adoption and direct-effect explanations of digital transformation in MSMEs.

METHOD

Proposed Empirical Validation Strategy and Analytical Approach

This study develops a conceptual moderated-mediation framework linking Digital Transformation Capability (DTC) to Accounting Information Resilience (AIR) through AI-Driven Analytics Capability (AIAC), with Cybersecurity Governance (CSG) positioned as a moderating condition. To provide a structured basis for future empirical validation, the study specifies a proposed quantitative explanatory design using a cross-sectional survey approach. Under this proposed design, the unit of analysis would be the firm, while the unit of observation would be a key informant with sufficient knowledge of the firm's accounting, financial, managerial, and digital technology processes. No observed survey data are analyzed in the present study; therefore, the empirical procedures described below should be interpreted as a proposed validation strategy rather than as completed field procedures.

Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4 is proposed for future empirical testing because the conceptual model contains multiple latent constructs, direct and indirect relationships, moderation effects, and moderated mediation. The proposed analysis would proceed in two stages consisting of measurement model assessment followed by structural model assessment, in accordance with the procedures recommended by Hair et al. (2022). The benchmark values presented in the analytical illustration are used solely to demonstrate how the proposed relationships could be evaluated and should not be interpreted as results obtained from actual respondents.

Proposed Population, Sampling Strategy, and Respondent Criteria

The proposed empirical validation would focus on micro, small, and medium-sized enterprises (MSMEs) operating in Pontianak City, West Kalimantan, Indonesia. Based on official 2023 data, the relevant MSME population consists of 28,128 business units distributed across six districts. Future empirical data collection would employ purposive sampling to identify firms with sufficient exposure to digital technologies and the organizational knowledge required to provide information about accounting, analytical, and cybersecurity practices.

Eligible firms would be required to operate in Pontianak City, have been in operation for at least two years, use at least one digital system for transactions, accounting, point-of-sale activities, inventory management, cloud-based bookkeeping, marketplace management, or financial administration, and process or store financial data digitally. Proposed respondents would include business owners, managers, finance or accounting personnel, or employees responsible for digital systems who possess adequate knowledge of the firm's financial and technological processes. These criteria represent the intended sampling and eligibility framework for future

empirical validation and do not indicate that respondents have already been recruited for the present conceptual study.

Construct Operationalization and Proposed Measurement

The four constructs are operationalized at the organizational level using multi-item measures adapted from prior research. DTC is conceptually developed from Khin and Ho (2019), Sousa-Zomer et al. (2020), and Warner and Wäger (2019). AIAC is adapted from Gupta and George (2016), Mikalef et al. (2020), and Mikalef and Gupta (2021). AIR is developed from He et al. (2022), Song et al. (2026), Huong and Dinh (2026), and Maldonado et al. (2026), while CSG is adapted from Wong et al. (2022), Hoong and Rezania (2024), and Nhan et al. (2025).

DTC encompasses digital integration, process redesign, resource reconfiguration, digital strategy, and data-enabled routines. AIAC includes AI-enabled analysis, pattern recognition, forecasting, analytical automation, data interpretation, and decision support. AIR captures the integrity, availability, continuity, adaptability, and recoverability of accounting information, whereas CSG includes cybersecurity responsibility, policies, access control, risk monitoring, data protection, incident response, and managerial oversight. In future empirical validation, all indicators would be assessed using a seven-point Likert scale ranging from 1 = strongly disagree to 7 = strongly agree.

Proposed Measurement Model Assessment

For future empirical testing, the measurement model would be evaluated to establish construct reliability and validity before interpretation of the structural relationships. Indicator reliability would be assessed using outer loadings, while internal consistency reliability would be examined using Cronbach's alpha, rho_A, and composite reliability. Values of 0.70 or higher would be considered acceptable. Convergent validity would be evaluated using Average Variance Extracted (AVE), with values above 0.50 indicating adequate convergence, while discriminant validity would be examined using the Heterotrait-Monotrait Ratio (HTMT).

Collinearity would be assessed using the Variance Inflation Factor (VIF) prior to interpretation of the structural path coefficients. In future survey implementation, potential common method bias would be reduced through neutral questionnaire wording, separation of predictor and outcome constructs, respondent confidentiality, and appropriate questionnaire design procedures. The benchmark measurement statistics presented in this study serve only as an illustrative demonstration of these assessment procedures and do not represent observed measurement properties.

Proposed Structural Model Assessment and Hypothesis Testing

The proposed structural model would be evaluated using path coefficients, R^2, adjusted R^2, f^2, and predictive relevance measures. Statistical significance would be assessed through nonparametric bootstrapping with 10,000 resamples and 95% confidence intervals. H1 would examine the proposed relationship between DTC and AIR, H2 the relationship between DTC and AIAC, and H3 the relationship between AIAC and AIR.

H4 would assess the mediating role of AIAC in the proposed relationship between DTC and AIR through the specific indirect effect. H5 would test whether CSG moderates the relationship between AIAC and AIR through an AIAC × CSG interaction term. H6 would examine moderated mediation by evaluating whether the proposed indirect effect of DTC on AIR through AIAC varies across different levels of CSG. Conditional effects

would be examined at low, mean, and high levels of CSG using bootstrapped confidence intervals. In the present study, the benchmark coefficients associated with these relationships are included solely to illustrate the internal analytical logic of the proposed model rather than to provide empirical hypothesis tests.

Proposed Ethical Protocol and Data Confidentiality

Because the present study does not report data collected from human participants, the ethical procedures described here represent a protocol for future empirical validation. Participation in any subsequent survey would be voluntary and based on informed consent. Respondents would be informed about the purpose of the research, the confidentiality of their responses, and their right to discontinue participation without penalty.

Future data collection would not request sensitive information such as passwords, security credentials, individual customer financial records, confidential transaction data, or detailed technical system configurations. Respondent and firm information would be treated confidentially, anonymized where appropriate, and analyzed only in aggregate form for academic purposes. Any institutional ethical approval required for the future empirical phase should be obtained before respondent recruitment and data collection.

RESULTS AND DISCUSSION

RESULTS

Benchmark Sample Structure

The benchmark design assumes 300 digitally engaged MSMEs distributed proportionally across the six districts of Pontianak City. The largest allocation is assigned to Pontianak Barat, with 68 firms (22.67%), followed by Pontianak Timur with 65 firms (21.67%) and Pontianak Utara with 52 firms (17.33%). The allocation closely reflects the geographic distribution of the 2023 MSME population.

Table 1. Benchmark Sample Distribution

District	Population	Benchmark Sample	%
Pontianak Barat	6,336	68	22.67
Pontianak Timur	6,145	65	21.67
Pontianak Utara	4,846	52	17.33
Pontianak Selatan	4,346	46	15.33
Pontianak Kota	3,722	40	13.33
Pontianak Tenggara	2,733	29	9.67
Total	28,128	300	100.00

The benchmark respondent composition assigns 37.33% of observations to business owners, 27.33% to managers, 23.67% to finance or accounting personnel, and 11.67% to technology-related personnel. The assumed sectoral coverage includes retail and trade, food and beverage, professional and general services, manufacturing, logistics, hospitality, and digital services. These distributions were specified to reflect the heterogeneity of digitally engaged MSMEs in Pontianak City and should not be interpreted as observed sample characteristics until field data are available.

Descriptive Statistics

The benchmark descriptive statistics indicate mean scores above the midpoint of the seven-point scale for all four constructs. Digital Transformation Capability records the highest benchmark mean (M = 5.42), followed by Accounting Information Resilience (M = 5.36), AI-Driven Analytics Capability (M = 5.08), and Cybersecurity Governance (M = 4.91).

Table 2. Benchmark Descriptive Statistics

Construct	Mean	SD	Minimum	Maximum
Digital Transformation Capability	5.42	0.82	2.50	7.00
AI-Driven Analytics Capability	5.08	0.88	2.17	7.00
Accounting Information Resilience	5.36	0.79	2.67	7.00
Cybersecurity Governance	4.91	0.93	2.00	7.00

Within the benchmark specification, Cybersecurity Governance has the lowest average value among the four constructs. This numerical pattern is consistent with the theoretical assumption that governance practices may develop more slowly than digital adoption and analytical capability. However, this pattern should be empirically verified using observed survey data before substantive conclusions are drawn.

Measurement Model Assessment

Indicator Reliability

The benchmark measurement model produces standardized outer loadings ranging from 0.788 to 0.881. All loadings exceed the conventional threshold of 0.708, indicating satisfactory indicator reliability within the benchmark specification.

Table 3. Benchmark Indicator Loadings

Construct	Indicator	Loading
DTC	DTC1	0.823
DTC	DTC2	0.847
DTC	DTC3	0.792
DTC	DTC4	0.866
DTC	DTC5	0.811
DTC	DTC6	0.838
AIAC	AIAC1	0.804
AIAC	AIAC2	0.856
AIAC	AIAC3	0.881
AIAC	AIAC4	0.827
AIAC	AIAC5	0.792
AIAC	AIAC6	0.845
AIR	AIR1	0.829
AIR	AIR2	0.874
AIR	AIR3	0.818
AIR	AIR4	0.861

Construct	Indicator	Loading
AIR	AIR5	0.793
AIR	AIR6	0.846
CSG	CSG1	0.788
CSG	CSG2	0.832
CSG	CSG3	0.869
CSG	CSG4	0.814
CSG	CSG5	0.851
CSG	CSG6	0.806

Internal Consistency and Convergent Validity

The benchmark values for Cronbach's alpha, rho_A, and composite reliability are above 0.90 for all constructs. Average Variance Extracted values range from 0.684 to 0.701, exceeding the recommended minimum value of 0.50.

Table 4. Benchmark Reliability and Convergent Validity

Construct	Cronbach's α	rho_A	CR	AVE
DTC	0.909	0.913	0.930	0.689
AIAC	0.912	0.916	0.932	0.697
AIR	0.915	0.919	0.934	0.701
CSG	0.906	0.910	0.928	0.684

Taken together, the benchmark values satisfy conventional reliability and convergent-validity criteria. Nevertheless, these statistics remain illustrative until reproduced from the final empirical dataset.

Discriminant Validity

Discriminant validity was evaluated using the Heterotrait-Monotrait Ratio. All benchmark HTMT values are below 0.85, with the highest value of 0.781 occurring between AI-Driven Analytics Capability and Accounting Information Resilience.

Table 5. Benchmark HTMT Ratios

Construct	DTC	AIAC	AIR	CSG
DTC	—			
AIAC	0.748	—		
AIR	0.704	0.781	—	
CSG	0.586	0.612	0.664	—

The benchmark pattern indicates adequate separation among the four latent constructs. Empirical discriminant validity, however, must ultimately be established using observed data.

Collinearity Assessment

Benchmark inner-model VIF values range from 1.000 to 2.080 and therefore remain below the conservative threshold of 3.3.

Table 6. Benchmark Collinearity Assessment

Predictor	Endogenous Construct	VIF

Predictor	Endogenous Construct	VIF
DTC	AIAC	1.000
DTC	AIR	1.92
AIAC	AIR	2.08
CSG	AIR	1.44
AIAC × CSG	AIR	1.13

These values indicate that the benchmark structural coefficients are not mechanically driven by excessive predictor collinearity.

Structural Model Assessment

Coefficient of Determination

The benchmark structural model produces an R^2 of 0.446 for AI-Driven Analytics Capability and 0.624 for Accounting Information Resilience.

Table 7. Benchmark Coefficients of Determination

Endogenous Construct	R^2	Adjusted R^2
AI-Driven Analytics Capability	0.446	0.444
Accounting Information Resilience	0.624	0.618

Within the benchmark model, Digital Transformation Capability accounts for 44.6% of the variance in AI-Driven Analytics Capability. DTC, AIAC, CSG, and the interaction term jointly account for 62.4% of the variance in Accounting Information Resilience. These values indicate the intended explanatory strength of the benchmark specification but should not be interpreted as empirical explanatory power.

Effect Size

The benchmark effect-size estimates indicate a large DTC → AIAC effect, a medium AIAC → AIR effect, and smaller effects for DTC → AIR, CSG → AIR, and AIAC × CSG → AIR.

Table 8. Benchmark Effect Sizes

Relationship	f^2	Interpretation
DTC → AIAC	0.805	Large
DTC → AIR	0.073	Small
AIAC → AIR	0.214	Medium
CSG → AIR	0.067	Small
AIAC × CSG → AIR	0.036	Small

The benchmark structure therefore assigns the strongest incremental contribution to the DTC → AIAC relationship, followed by the contribution of AIAC to AIR.

Predictive Relevance

The benchmark Q^2 predict values are positive for both endogenous constructs.

Table 9. Benchmark Predictive Relevance

Construct	Q^2 predict
AIAC	0.431
AIR	0.572

The model also produces a benchmark SRMR value of 0.061. These statistics are numerically consistent with acceptable predictive and model-fit characteristics, but their empirical interpretation requires replication with observed survey data.

Direct Effect Assessment

Table 10. Benchmark Direct Effects

Hyp.	Relationship	β	SE	t	p	95% CI	Benchmark Outcome
H1	DTC → AIR	0.236	0.055	4.291	<0.001	[0.128, 0.342]	Consistent with H1
H2	DTC → AIAC	0.668	0.041	16.293	<0.001	[0.588, 0.746]	Consistent with H2
H3	AIAC → AIR	0.418	0.052	8.038	<0.001	[0.316, 0.518]	Consistent with H3

The largest benchmark path coefficient occurs between DTC and AIAC (β = 0.668), followed by AIAC → AIR (β = 0.418) and DTC → AIR (β = 0.236). The numerical structure therefore reflects the theoretical expectation that digital transformation primarily contributes to accounting-information resilience by strengthening analytical capability rather than through the direct pathway alone.

Mediation Assessment

The benchmark indirect effect of DTC on AIR through AIAC is β = 0.279, while the direct effect remains positive at β = 0.236.

Table 11. Benchmark Mediation Effects

Effect	β	SE	t	p	95% CI
DTC → AIAC → AIR	0.279	0.043	6.488	<0.001	[0.198, 0.366]
Direct DTC → AIR	0.236	0.055	4.291	<0.001	[0.128, 0.342]
Total DTC → AIR	0.515	0.048	10.729	<0.001	[0.423, 0.607]

Within the benchmark specification, the positive direct and indirect coefficients correspond to a complementary partial-mediation pattern. This pattern is consistent with H4 at the benchmark level, but empirical mediation should only be concluded after the indirect effect is reproduced from actual survey data.

Moderation Assessment

The benchmark model includes a positive main effect of CSG on AIR (β = 0.190) and a positive interaction between AIAC and CSG.

Table 12. Benchmark Moderation Effect

Interaction Effect	β	SE	t	p	95% CI	Benchmark Outcome
AIAC × CSG → AIR	0.137	0.047	2.915	0.004	[0.046, 0.228]	Consistent with H5

The positive benchmark interaction coefficient indicates the expected strengthening role of Cybersecurity Governance in the AIAC–AIR relationship.

Simple Slope Analysis

The benchmark conditional effects increase across low, mean, and high levels of Cybersecurity Governance.

Table 13. Benchmark Conditional Effects of AIAC on AIR

CSG Level	Conditional AIAC → AIR Effect
Low (−1 SD)	0.281
Mean	0.418
High (+1 SD)	0.555

The benchmark gradient indicates that the AIAC → AIR relationship becomes stronger as CSG increases. The conditional coefficient at high CSG is approximately twice that observed at low CSG, which is numerically consistent with the proposed moderating mechanism.

Moderated Mediation Assessment

The benchmark conditional indirect effect of DTC on AIR through AIAC increases across levels of Cybersecurity Governance.

Table 14. Benchmark Conditional Indirect Effects

Cybersecurity Governance	Conditional Indirect Effect	SE	t	p	95% CI
Low (−1 SD)	0.188	0.045	4.178	<0.001	[0.105, 0.281]
Mean	0.279	0.043	6.488	<0.001	[0.198, 0.366]
High (+1 SD)	0.371	0.056	6.625	<0.001	[0.268, 0.484]

The benchmark moderated-mediation index is β = 0.092 (SE = 0.030, t = 3.067, p = 0.002, 95% CI [0.036, 0.153]). Because the benchmark confidence interval excludes zero, the numerical pattern is consistent with the conditional indirect-effect proposition represented by H6.

At the benchmark level, the indirect pathway becomes progressively stronger as Cybersecurity Governance increases. This pattern corresponds to the theoretical proposition that AI-enabled analytical capability translates digital transformation into greater accounting-information resilience more effectively when supported by stronger cybersecurity governance.

Importance – Performance Map Analysis

The benchmark Importance – Performance Map Analysis indicates different combinations of importance and performance across the three focal antecedent constructs.

Table 15. Benchmark Importance–Performance Map Analysis

Construct	Importance for AIR	Performance
Digital Transformation Capability	0.515	74.2
AI-Driven Analytics Capability	0.418	72.8
Cybersecurity Governance	0.190	68.4

Within the benchmark specification, Cybersecurity Governance records the lowest performance score, whereas Digital Transformation Capability has the highest importance value. This benchmark pattern identifies CSG as a potential area of managerial attention, although such prioritization should be confirmed with empirical IPMA results before managerial recommendations are finalized.

Summary of Benchmark Hypothesis Assessment

Table 16. Summary of Benchmark Hypothesis Assessment

Relationship	Benchmark Outcome
DTC → AIR	Consistent with hypothesis
DTC → AIAC	Consistent with hypothesis
AIAC → AIR	Consistent with hypothesis
DTC → AIAC → AIR	Consistent with complementary mediation
AIAC × CSG → AIR	Consistent with moderation hypothesis
Moderated mediation	Consistent with conditional indirect-effect hypothesis

Taken together, the benchmark model specifies a coherent moderated-mediation structure. DTC has its strongest benchmark association with AIAC (β = 0.668), while AIAC is positively related to AIR (β = 0.418). The benchmark direct DTC → AIR coefficient is smaller (β = 0.236), and the benchmark indirect effect through AIAC is β = 0.279. In addition, the AIAC × CSG interaction is positive (β = 0.137), and the conditional indirect effect increases from 0.188 at low CSG to 0.371 at high CSG.

These values demonstrate the internal numerical logic of the proposed benchmark model, but they should not be presented as empirical findings or as evidence that H1–H6 are supported until they are replaced by reproducible outputs derived from the actual survey dataset.

Discussion

The benchmark analytical pattern provides a theoretically coherent representation of how Digital Transformation Capability (DTC), AI-Driven Analytics Capability (AIAC), Cybersecurity Governance (CSG), and Accounting Information Resilience (AIR) may operate within an integrated capability-based framework. Rather than interpreting the benchmark coefficients as empirical confirmation, the discussion evaluates whether the numerical pattern is theoretically consistent with the proposed relationships and existing research. Particular attention is given to the mechanisms linking digital transformation with accounting information resilience, the mediating role of AI-driven analytics, the conditioning role of cybersecurity governance, and the organizational circumstances under which these relationships may become stronger or weaker.

Digital Transformation Capability, AI-Driven Analytics Capability, and Accounting Information Resilience

The benchmark model assigns the strongest structural relationship to DTC → AIAC (β = 0.668), while the direct DTC → AIR relationship is comparatively smaller (β = 0.236). This pattern is consistent with the theoretical expectation that digital transformation creates value primarily by establishing the organizational conditions required for more specialized capabilities to develop. Digital transformation therefore represents more than the acquisition of digital technologies; it involves the coordinated reconfiguration of technologies, data, human competencies, and organizational routines (Vial, 2019; Warner & Wäger, 2019; Sousa-Zomer et al., 2020).

For digitally engaged MSMEs, such a capability may provide the infrastructure necessary for integrated data processing, automated accounting activities, and more responsive financial-information routines. The benchmark pattern is therefore consistent with H1 and H2, but it should not yet be interpreted as empirical

confirmation. An alternative explanation is that firms with greater organizational maturity, managerial capability, or financial resources may simultaneously exhibit stronger digital transformation, analytics capability, and accounting resilience. Firm size, digital maturity, and accumulated technological experience may therefore represent important boundary conditions when the model is tested empirically.

The benchmark relationship between AIAC and AIR (β = 0.418) further indicates the theoretical importance of analytical capability for resilient accounting-information processes. AI-enabled analytics can potentially strengthen anomaly detection, forecasting, reconciliation, exception monitoring, and managerial response, thereby increasing the capacity of accounting systems to preserve integrity, continuity, adaptability, and recoverability under disruption. This interpretation is compatible with analytics-capability research showing that analytical resources generate organizational value when they are integrated with human knowledge, organizational routines, and decision-making processes (Gupta & George, 2016; Mikalef & Gupta, 2021).

However, AI-enabled analytics should not be assumed to generate resilience automatically. Its effectiveness may depend on data quality, interoperability among digital systems, employee analytical skills, and managerial willingness to use analytical outputs. In MSMEs, these conditions may be especially important because AI functionality is often accessed through external platforms, accounting applications, payment systems, or cloud services rather than proprietary AI infrastructure. Thus, the proposed AIAC–AIR relationship should be interpreted as organizationally contingent rather than technologically deterministic.

AI-Driven Analytics Capability as a Mediating Mechanism

The benchmark indirect effect of DTC on AIR through AIAC is β = 0.279, while the direct DTC → AIR coefficient remains positive. Numerically, this configuration corresponds to complementary partial mediation and is consistent with the theoretical proposition represented by H4. More importantly, it provides a process explanation for the proposed relationship between digital transformation and accounting information resilience. DTC establishes digital infrastructure, integrated processes, and data availability, whereas AIAC represents a more proximal information-processing capability through which these resources can be transformed into actionable insights.

This interpretation extends previous research that associates digital transformation with organizational resilience (He et al., 2022) and accounting information quality (Song et al., 2026) by specifying an analytical mechanism between digital transformation and the resilience of accounting information. It is also consistent with research suggesting that analytical technologies create organizational value through intermediate capabilities rather than through technology ownership alone (Mikalef et al., 2020). Nevertheless, alternative pathways remain possible. Digital transformation may strengthen AIR through process standardization, cloud redundancy, automated controls, employee digital competence, or improvements in accounting information-system quality independently of AIAC. Empirical analysis should therefore determine the relative importance of AIAC compared with these alternative mechanisms rather than assuming that analytics constitutes the only conversion pathway.

Cybersecurity Governance as a Boundary Condition

The benchmark interaction between AIAC and CSG is positive (β = 0.137), while the conditional AIAC → AIR coefficient increases from 0.281 at low CSG to 0.555 at high CSG. This numerical pattern is consistent with H5 and with the theoretical argument that cybersecurity governance may amplify the resilience benefits associated with AI-driven analytics. Analytical capability relies on access to interconnected digital information; consequently, its potential benefits can be undermined when data integrity, access privileges, incident-response responsibilities, or recovery mechanisms are inadequately governed.

This interpretation is consistent with research that conceptualizes cybersecurity as an organizational and governance issue rather than exclusively a technical safeguard. Hoong and Rezania (2024) emphasize the organizational foundations of cybersecurity governance in smaller firms, while Nhan et al. (2025) show that accounting information security controls are influenced by organizational, technological, and policy-related conditions. In this sense, CSG can be understood as a boundary condition that determines whether analytical capability operates within an information environment sufficiently protected to support resilient accounting processes.

The moderating relationship should nevertheless be interpreted cautiously. Stronger cybersecurity governance may itself reflect broader managerial professionalism, formalization, or organizational maturity. It is therefore possible that firms with more developed governance structures simultaneously maintain stronger analytical capabilities and more resilient accounting processes. Moreover, the importance of CSG may vary by industry, digital intensity, and exposure to cyber threats. Cybersecurity governance may be particularly consequential for MSMEs that depend heavily on cloud platforms, digital payments, marketplaces, or interconnected information systems, whereas its marginal influence may differ in less digitally intensive business environments.

Moderated Mediation and Capability Complementarity

The benchmark conditional indirect effect increases from 0.188 at low CSG to 0.371 at high CSG, with a moderated-mediation index of β = 0.092. Rather than being treated as empirical proof, this pattern illustrates the theoretical logic underlying H6: the proposed indirect effect of DTC on AIR through AIAC becomes stronger when cybersecurity governance is more developed. The model therefore moves beyond a simple assumption that increasing digitalization necessarily produces greater organizational resilience.

The central implication is one of capability complementarity. Digital transformation provides the digital and organizational foundation, AI-driven analytics provides the capacity to interpret and respond to information, and cybersecurity governance provides the institutional safeguards that protect the environment in which analytical activities occur. These capabilities may therefore generate greater value when developed jointly rather than independently. This reasoning is particularly relevant to resource-constrained MSMEs, where investment decisions often require prioritization among technology, analytical competence, and security governance.

At the same time, capability complementarity represents a boundary condition rather than a universal relationship. The relative importance of DTC, AIAC, and CSG

may differ according to firm size, industry, digital maturity, managerial expertise, and prior exposure to operational or cybersecurity disruptions. For less digitally mature MSMEs, basic system integration and reliable digital recordkeeping may remain more important than advanced AI-enabled analytics. Conversely, as digital dependence increases, cybersecurity governance may become progressively more important because disruptions can affect increasingly interconnected accounting-information processes.

Theoretical Implications

The proposed model contributes to the literature in three related ways. First, it distinguishes Accounting Information Resilience from conventional accounting information quality by emphasizing the ability of accounting-information processes to preserve or restore integrity, availability, continuity, adaptability, and recoverability under disruption. This distinction shifts the theoretical focus from the quality of information under stable operating conditions to the robustness of information processes under adverse conditions.

Second, the model identifies AIAC as a theoretically plausible conversion mechanism between DTC and AIR. This extends capability-based explanations of digital transformation by specifying how digital resources may be converted into more adaptive information-processing routines. Third, the framework positions CSG as a boundary condition rather than merely another antecedent of information quality or security. The combination of mediation and moderation therefore provides an integrated explanation of both how digital transformation may generate accounting-information resilience and under what governance conditions this mechanism may become more effective.

Managerial Implications

For MSME managers, the framework suggests that digital transformation should not be reduced to investments in software, cloud platforms, digital payments, automated bookkeeping, or AI-enabled applications. Digital investments are more likely to strengthen accounting-information resilience when they are accompanied by organizational routines that support analytical use and governance arrangements that protect the underlying information environment

The benchmark Importance–Performance Map Analysis also identifies CSG as the construct with the lowest performance score (68.4), compared with DTC (74.2) and AIAC (72.8). Although these values remain benchmark indicators rather than empirical managerial evidence, they highlight a theoretically relevant issue: MSMEs may develop digital and analytical capabilities more rapidly than formal cybersecurity governance. A balanced digital-transformation strategy should therefore integrate digital process development, analytical capability, access control, data protection, cybersecurity accountability, incident-response procedures, and recovery planning rather than treating cybersecurity as a technical activity undertaken after digital systems have already been implemented.

Overall Interpretation

Overall, the benchmark model is theoretically consistent with an integrated capability-governance explanation of accounting information resilience. The proposed relationships suggest that DTC may establish the foundation for AIAC, AIAC may provide the mechanism through which digital resources are translated into AIR, and

CSG may determine how effectively this conversion occurs. The framework therefore offers a more conditional explanation than a direct technology–outcome model.

However, these interpretations remain theoretical expectations supported by the internal logic of the benchmark model rather than demonstrated empirical findings. Consequently, statements regarding hypothesis support, causal strength, and managerial priorities should ultimately be based on reproducible results from observed MSME data. Future empirical testing should also examine whether the proposed relationships vary across firm size, industry, digital maturity, employee competence, data quality, and exposure to cybersecurity risks.

CONCLUSIONS

This study develops an integrated capability-based framework linking Digital Transformation Capability (DTC), AI-Driven Analytics Capability (AIAC), Cybersecurity Governance (CSG), and Accounting Information Resilience (AIR) in digitally engaged MSMEs. The framework proposes that DTC provides the organizational and technological foundation for developing AIAC, while AIAC represents a potential mechanism through which digital resources may be translated into more resilient accounting-information processes. CSG is positioned as a boundary condition that may strengthen this mechanism by supporting data integrity, access control, cybersecurity accountability, incident response, and recovery. By integrating these relationships within a moderated-mediation framework, the study extends technology–outcome perspectives and conceptually distinguishes AIR from conventional accounting information quality through its emphasis on integrity, availability, continuity, adaptability, and recoverability under disruption. From a managerial perspective, the framework suggests that digital technology investment should be considered alongside analytical capability development and cybersecurity governance rather than as an isolated initiative. However, the numerical values presented in this study are benchmark-based and are intended only to illustrate the internal analytical logic of the proposed model; they should not be interpreted as empirical confirmation of the hypothesized relationships. Future research should therefore validate the framework using observed MSME data and examine whether the proposed relationships vary across firm size, industry, digital maturity, and cybersecurity exposure. Longitudinal and multi-informant designs may also provide stronger evidence regarding how accounting information resilience develops and changes over time.

AKNOWLEDGMENT

The authors gratefully acknowledge the academic support provided by Institut Bisnis dan Ekonomi Indonesia and Politeknik Negeri Pontianak during the development of this manuscript. The authors also appreciate the constructive insights and academic assistance provided by colleagues and other parties who contributed to the refinement of the conceptual framework and manuscript.

AUTHOR CONTRIBUTION STATEMENT

NA contributed to the conceptualization, theoretical development, methodological design, analytical framework, and manuscript preparation. MA contributed to the conceptual research design, literature review, and critical revision of the manuscript. TA contributed to the development of the proposed measurement framework, methodological refinement, and manuscript editing. LN contributed to the theoretical

discussion, validation of the conceptual framework, and manuscript review. AVLO contributed to academic supervision, critical evaluation, and final manuscript revision. All authors reviewed and approved the final version of the manuscript.

AI DISCLOSURE STATEMENT

The authors used ChatGPT (OpenAI) during manuscript preparation to support language refinement, improve textual clarity, and enhance the organization of selected sections. All AI-assisted outputs were critically reviewed, revised, and verified by the authors before inclusion in the manuscript. The authors retain full responsibility for the conceptual arguments, interpretation of the literature, analytical framework, accuracy of citations, and conclusions presented in this work.

REFERENCES

Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? International Journal of Production Economics, 182, 113–131. doi:10.1016/j.ijpe.2016.08.018

Al Shanti, A. M., & Elessa, M. S. (2023). The impact of digital transformation towards blockchain technology application in banks to improve accounting information quality and corporate governance effectiveness. Cogent Economics & Finance, 11(1), 2161773. doi:10.1080/23322039.2022.2161773

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers & Industrial Engineering, 149, 106829. doi:10.1016/j.cie.2020.106829

Awolowo, I. F., Ode, E., Abidoye, A., Ajao, O., & Jogunola, O. (2026). Cybersecurity assurance for SMEs: A conceptual framework integrating organizational culture, fraud risk management and forensic accounting. Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration, 43(1), e70051. doi:10.1002/cjas.70051

Diah, A. M., Hasiara, L. O., Lesmana, D., Raharjo, S., Aprianti, Y., & Yudaruddin, R. (2026). Information technology capability and financial reporting quality in local governments: The mediating role of accounting information system quality. Cogent Business & Management, 13(1), 2654816. doi:10.1080/23311975.2026.2654816

Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Pontianak. (2026, June 18). Dekatkan layanan dan permudah legalitas, DPMPTSP Kota Pontianak gelar sosialisasi dan pendampingan OSS bagi pelaku UMKM di Kecamatan Pontianak Selatan. DPMPTSP Kota Pontianak

Dubey, R., Gunasekaran, A., & Childe, S. J. (2019). Big data analytics capability in supply chain agility: The moderating effect of organizational flexibility. Management Decision, 57(8), 2092–2112. doi:10.1108/MD-01-2018-0119

Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. Journal of Strategy and Management, 15(2), 272–286. doi:10.1108/JSMA-04-2021-0089

Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2022). Artificial intelligence and business value: A literature review. Information Systems Frontiers, 24, 1709–1734. doi:10.1007/s10796-021-10186-w

Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. A. (2024). Cybersecurity resilience in SMEs: A machine learning approach. Journal of Computer Information Systems, 64(6), 711–727. doi:10.1080/08874417.2023.2248925

Gupta, M., & George, J. F. (2016). Toward the development of a big data analytics capability. Information & Management, 53(8), 1049–1064. doi:10.1016/j.im.2016.07.004

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808–834. doi:10.1108/MAJ-09-2018-2004

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). SAGE Publications.

Haj Mohammadi, B., J. Sadeghi, V., Sukumar, A., & Mmadubuko, M. (2026). Cybersecurity as a dynamic capability: How micro and small social enterprises build digital resilience. Information Systems Frontiers. Advance online publication. doi:10.1007/s10796-026-10718-2

He, Z., Huang, H., Choi, H., & Bilgihan, A. (2022). Building organizational resilience with digital transformation. Journal of Service Management, 34(1), 147–171. doi:10.1108/JOSM-06-2021-0216

Hoong, Y., & Rezania, D. (2024). Navigating cybersecurity governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises. Computers & Security, 142, 103852. doi:10.1016/j.cose.2024.103852

Huong, N. T., & Dinh, D. V. (2026). Accounting information systems and business capabilities' role impacting the Viet Nam-listed corporates' resilience: The smart-PLS SEM approach. Journal of Accounting & Organizational Change, 22(3), 430–453. doi:10.1108/JAOC-07-2024-0250

Khin, S., & Ho, T. C. F. (2019). Digital technology, digital capability and organizational performance: A mediating role of digital innovation. International Journal of Innovation Science, 11(2), 177–195. doi:10.1108/IJIS-08-2018-0083

Maldonado, I., Ferreira-da-Silva, A., Pinho, C., & Santos, G. (2026). Cybersecurity in accounting: Challenges and strategies for SME resilience. Journal of Accounting & Organizational Change. Advance online publication. doi:10.1108/JAOC-07-2025-0267

Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. Information & Management, 58(3), 103434. doi:10.1016/j.im.2021.103434

Mikalef, P., Krogstie, J., Pappas, I. O., & Pavlou, P. A. (2020). Exploring the relationship between big data analytics capability and competitive performance: The mediating roles of dynamic and operational capabilities. Information & Management, 57(2), 103169. doi:10.1016/j.im.2019.05.004

Nhan, V. T. T., Dung, N. N. K., & Tran, P. (2025). A study on the impact of accounting information security controls on the effectiveness of internal controls in Vietnamese enterprises. Journal of Open Innovation: Technology, Market, and Complexity, 11(1), 100470. doi:10.1016/j.joitmc.2025.100470

Ode, E., Awolowo, I. F., Nana, R., & Olawoyin, F. S. (2025). Social capital and artificial intelligence readiness: The mediating role of cyber resilience and value construction of SMEs in resource-constrained environments. Information Systems Frontiers. Advance online publication. doi:10.1007/s10796-025-10608-z

Omrani, N., Rejeb, N., Maalaoui, A., Dabić, M., & Kraus, S. (2024). Drivers of digital transformation in SMEs. IEEE Transactions on Engineering Management, 71, 5030–5043. doi:10.1109/TEM.2022.3215727

Omrani, N., Wilke, B., Kraus, S., & Kanbach, D. K. (2026). Cybersecurity strategies in European SMEs: Navigating digital risks and enhancing cyber resilience. Information Systems Frontiers. Advance online publication. doi:10.1007/s10796-026-10801-8

Pemerintah Kota Pontianak. (2024). Peraturan Daerah Kota Pontianak Nomor 3 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Daerah Tahun 2025–2045. Dokumen resmi Pemerintah Kota Pontianak

Pemerintah Kota Pontianak. (2026a, March 9). 30 UMKM di Pontianak ikut pelatihan pengelolaan keuangan digital. Pemerintah Kota Pontianak

Pemerintah Kota Pontianak. (2026b, August 16). QRIS perluas ekosistem digital. Pemerintah Kota Pontianak

Rialti, R., Zollo, L., Ferraris, A., & Alon, I. (2019). Big data analytics capabilities and performance: Evidence from a moderated multi-mediation model. Technological Forecasting and Social Change, 149, 119781. doi:10.1016/j.techfore.2019.119781

Rupeika-Apoga, R., Petrovska, K., & Bule, L. (2022). The effect of digital orientation and digital capability on digital transformation of SMEs during the COVID-19 pandemic. Journal of Theoretical and Applied Electronic Commerce Research, 17(2), 669–685. doi:10.3390/jtaer17020035

Sahoo, S., Kumar, S., Donthu, N., & Singh, A. K. (2024). Artificial intelligence capabilities, open innovation, and business performance: Empirical insights from multinational B2B companies. Industrial Marketing Management, 117, 28–41. doi:10.1016/j.indmarman.2023.12.008

Song, H., Lu, Y., & Yang, Z. (2026). Digital transformation of enterprises and accounting information quality: A resource dependence theory perspective. Emerging Markets Finance and Trade, 62(5), 1328–1344. doi:10.1080/1540496X.2025.2552882

Sousa-Zomer, T. T., Neely, A., & Martinez, V. (2020). Digital transforming capability and performance: A microfoundational perspective. International Journal of Operations & Production Management, 40(7/8), 1095–1128. doi:10.1108/IJOPM-06-2019-0444

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889–901. doi:10.1016/j.jbusres.2019.09.022

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144. doi:10.1016/j.jsis.2019.01.003

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356–365. doi:10.1016/j.jbusres.2016.08.009

Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. Long Range Planning, 52(3), 326–349. doi:10.1016/j.lrp.2018.12.001

Wei, R., & Pardo, C. (2022). Artificial intelligence and SMEs: How can B2B SMEs leverage AI platforms to integrate AI technologies? Industrial Marketing Management, 107, 466–483. doi:10.1016/j.indmarman.2022.10.008

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management, 66, 102520. doi:10.1016/j.ijinfomgt.2022.102520

Yigit Ozkan, B., & Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. Journal of Computer Information Systems, 63(4), 965–987. doi:10.1080/08874417.2022.2119442