



Publisher

<http://jssidoi.org/esc/home>

ENTERPRISE DIGITAL RESILIENCE CAPABILITY FRAMEWORK: AN INTEGRATED DYNAMIC CAPABILITY APPROACH*

Viktoriia Hrosul ¹, Volodymyr Yermachenko ², Serhii Zubkov ³, Alina Kolesnyk ⁴, Marek Semerád ⁵

^{1,3,4} State Biotechnological University, Ukraine, Alchevskih str.44, 61002 Kharkiv, Ukraine

² Simon Kuznets Kharkiv National University of Economics, Av. Nayka 9-A, 161166 Kharkiv, Ukraine

^{2,5} Bratislava University of Economics and Management, Furdekova 16, 85104 Bratislava, Slovak Republic

E-mails: ¹viktoriagrosul@gmail.com; ²Volodymyr.yermachenko@vsem.sk; ³s.zubkov@biotechuniv.edu.ua

⁴lala4ka@ukr.net; ⁵marek.semerad@artendr.cz

Received 25 August 2025; accepted 18 November 2025; published 30 December 2025

Abstract. This paper addresses how organisations can develop integrated capabilities to withstand digital disruptions while leveraging them strategically. Three critical gaps are identified: treating digital risk management operationally rather than strategically, using inadequate linear risk models, and lacking practical implementation guidance. The research develops a comprehensive framework integrating dynamic capabilities theory with enterprise resilience, establishes measurable constructs, and provides a practical maturity model. A multi-stage conceptual development methodology was employed: systematic literature integration across digital transformation, enterprise resilience, and dynamic capabilities; iterative framework development; expert validation using modified Delphi methodology with 12 experts achieving strong agreement ($\kappa=0.83$); and implementation roadmap creation for different maturity levels. The Digital Resilience Capability Framework establishes relationships between three components—Anticipatory Intelligence System, Adaptive Response Architecture, and Strategic Transformation Capability—mapping to Teece's sensing-seizing-reconfiguring taxonomy. Six integration pathways create a cohesive system exhibiting recursive learning, temporal integration, cross-boundary integration, and value amplification. The Digital Resilience Maturity Matrix formalises resilience as evolving through five progressive levels from Reactive to Transformative. This research addresses theoretical triangulation by integrating dynamic capabilities theory, complex adaptive systems, and enterprise resilience. It operationalises how dynamic capabilities enable digital resilience and reconceptualises resilience as a strategic meta-capability, challenging risk-avoidance paradigms. Complex adaptive systems principles explain how component interactions generate amplified resilience value. The framework provides structured capability development, balancing immediate mitigation with long-term advantage. The maturity matrix enables precise diagnostic assessment while integration mechanisms ensure cohesive system functionality. The Digital Value Resilience Ratio quantifies strategic benefits beyond risk avoidance, strengthening business cases for resilience investments.

Keywords: digital resilience; dynamic capabilities; digital transformation; enterprise risk management; capability maturity; strategic resilience; organisational adaptation.

Reference to this paper should be made as follows: Hrosul, V., Yermachenko, V., Zubkov, S., Kolesnyk, A., Semerád, M. 2025. Enterprise digital resilience capability framework: an integrated dynamic capability approach. *Entrepreneurship and Sustainability Issues*, 13(2), 399-416. <http://doi.org/10.9770/e4483987593>

JEL Classifications: O33, M15, L21, D83, M21

* This research was funded by the EU Next Generation EU through the Recovery and Resilience Plan for Slovakia under the project No. 09I03-03-V01-00133

1. Introduction

Digital transformation has evolved from a technological initiative into a fundamental strategic imperative that reshapes modern organisations. While offering unprecedented opportunities for value creation, this transformation simultaneously introduces complex vulnerabilities through increased system interconnectedness, data dependencies, and operational complexity. Organisations face a critical paradox: the very technologies driving competitive advantage also amplify enterprise vulnerability, creating what might be termed a "digital resilience dilemma".

Despite the growing recognition of this challenge, organisations continue to struggle with effectively managing digital risks. Recent industry data reveals a sobering reality – 68% of digital transformation initiatives fail (Gartner, 2023), with "inadequate risk resilience architecture" identified as a primary contributing factor. This statistic underscores not merely implementation challenges but a fundamental conceptual gap in how organisations approach the intersection of digital transformation and resilience.

A critical analysis of existing literature reveals three significant gaps that hinder organisational capability development in this domain:

First, current approaches treat digital risk management primarily as an operational consideration rather than a strategic capability. This creates a fundamental disconnect between transformation initiatives and resilience mechanisms, often resulting in what is described as "digital transformation myopia" – the failure to anticipate second-order effects of technological change.

Second, traditional risk management frameworks employ linear, event-based models that prove inadequate in digital environments characterised by emergence and complexity. These conventional frameworks operate on the assumption that risks can be comprehensively identified and mitigated before materialisation, an assumption increasingly challenged in rapidly evolving digital contexts (Androniceanu, 2024a; Androniceanu & Colesca, 2025).

Third, a significant chasm exists between theoretical resilience models and practical implementation guidance. This gap is particularly pronounced for organisations at different digital maturity stages, leading to what Liu (2024), Androniceanu (2024b), and Androniceanu (2025a) identify as the "capability development gap" in digital transformation initiatives.

The significance of addressing these gaps extends beyond academic contribution to urgent practical needs. As organisations increasingly depend on digital infrastructure and capabilities, their exposure to systemic digital risks grows proportionally. Without integrated frameworks that simultaneously address transformation imperatives and resilience requirements, organisations face continuing high failure rates in their digital initiatives (Androniceanu, 2025b).

This research addresses a fundamental question: How can organisations develop integrated capabilities that enable them not only to withstand digital disruptions but to leverage them as catalysts for sustainable competitive advantage? This question challenges the prevailing risk-avoidance paradigm by reconceptualising resilience as a value-creating strategic capability rather than merely a defensive posture.

We establish a novel theoretical bridge between dynamic capabilities theory and enterprise resilience through an integrated conceptual framework. Dynamic capabilities – defined as "the firm's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments" (Teece, 2007) – provide an ideal theoretical lens for understanding digital resilience (Craciun et al., 2025). This connection is operationalised through three capability dimensions that directly map to Teece's sensing-seizing-reconfiguring taxonomy:

1. Sensing → Anticipatory Intelligence System (AIS) – enhancing the organisation's ability to detect weak signals of emerging digital risks before they materialise as disruptions.

2. Seizing → Adaptive Response Architecture (ARA) – developing the structural and process capabilities to rapidly mobilise resources in response to digital disruptions.
3. Reconfiguring → Strategic Transformation Capability (STC) – building the strategic flexibility to convert disruptions into opportunities through organisational learning and business model innovation.

This theoretical integration advances Pavlou P. and Sawy's O. (Pavlou & Sawy, 2011) work on dynamic capabilities by specifically extending their application to digital resilience contexts, addressing what Liu Y. (Liu, 2024) describes as the "strategic agility gap" in digital transformation initiatives.

This paper pursues three interconnected objectives:

1. Develop a comprehensive conceptual framework that integrates dynamic capabilities theory with enterprise resilience in digital transformation contexts
2. Articulate measurable constructs and their relationships within this framework, enabling empirical validation
3. Provide a practical maturity model and implementation roadmap for organisations at different stages of digital transformation

2. Literature Review

2.1. Digital Transformation Strategic Imperative and Risk Landscape

Digital transformation has evolved from a technological consideration to a fundamental strategic imperative, reshaping organisational structures, business models, and competitive dynamics. The literature reveals three distinct conceptualisations of this phenomenon:

1. Technological Perspective. Early research primarily framed digital transformation as technology adoption (Fitzgerald et al., 2014; Kane, 2019), focusing on implementation challenges while largely overlooking strategic resilience implications..
2. Organisational Change Perspective. Recent literature recognises the profound organisational changes triggered by digital initiatives. Cao et al. (2025) emphasise that digital transformation requires "the integration of digital strategy, digital skills, and the use of digital technologies across all organisational domains," establishing transformation as a multi-dimensional organisational challenge rather than simply technological adoption. According to the authors, digital transformation entails a comprehensive renewal of business models, processes, and organisational structures, achieved through the synergy of organisational and social factors.
3. Strategic Disruption Perspective. Contemporary research increasingly frames digital transformation as a strategic disruption, with Liu (2024) noting that external pressures, such as competitive advantage and cost efficiency, drive transformation while simultaneously introducing systemic vulnerabilities. This perspective aligns with Vial's (2019) meta-analysis finding that 68% of transformation initiatives create unintended organisational disruptions that current frameworks inadequately address.

Our critical analysis reveals a significant gap: while digital transformation literature acknowledges associated risks, it typically treats them as implementation hurdles rather than strategic variables requiring dedicated capability development. This fragmentation is evidenced by the absence of integrated frameworks addressing both transformation enablement and resilience building simultaneously.

2.2. Enterprise Risk Management and Resilience

The evolution of enterprise risk management (ERM) literature reveals a trajectory from protection-focused approaches toward adaptive resilience paradigms, though significant conceptual limitations persist:

Traditional ERM Limitations. Conventional risk management frameworks (COSO, 2017; ISO 31000, 2018) employ event-based, linear models ill-equipped for digital environments characterised by complexity and emergence. These frameworks operate on the assumption that risks can be comprehensively identified and mitigated before materialisation.

Resilience as Organizational Capability. More recent literature conceptualises resilience as an organisational capability rather than a risk outcome. Williams et al. (2017) define organisational resilience as "the capacity to

anticipate and respond to disruptions through adaptive behaviours," emphasising proactive sensing over reactive response – a critical distinction for digital environments characterised by rapid change and interconnectedness.

Digital Context Adaptation Deficit. Despite these advances, Saeed et al. (2023) identify a critical limitation: existing resilience frameworks remain insufficiently adapted to digital transformation contexts. Their empirical analysis of cybersecurity resilience demonstrates that conventional frameworks fail to account for the unique characteristics of digital risks, including:

1. Systemic interdependencies between technological and organisational elements.
2. Non-linear escalation patterns defying traditional probability assessment.
3. Compressed response timelines requiring automated decision protocols.

This analysis reveals a second research gap: while resilience literature has evolved toward capability-based conceptualisations, it lacks integrated frameworks specifically adapted to digital transformation contexts. This gap manifests in practice as what Xiao et al. (2023) term the "digital resilience paradox" – organisations simultaneously increasing digital dependencies while underinvesting in commensurate resilience capabilities.

2.3. Dynamic Capabilities as Theoretical Foundation for Digital Resilience

Dynamic capabilities theory offers a robust foundation for understanding how organisations can develop sustainable resilience in rapidly changing digital environments.

Teece's (2007) framework of sensing, seizing, and reconfiguring capabilities provides an architectural template for understanding organisational adaptation. Critically, Pavlou and Sawy (2011) extended this framework by operationalising dynamic capabilities into measurable constructs – a crucial advancement for empirical validation.

Recent literature has begun applying dynamic capabilities theory to digital contexts. Warner and Wäger (2019) identified digital sensing capability and digital seizing capability as distinct dynamic capabilities enabling sustainable transformation. However, their analysis focuses primarily on opportunity exploitation rather than integrated resilience development.

Garzoni et al. (2020) advanced understanding of capability micro-foundations by examining how SMEs develop digital transformation capabilities across maturity stages. Their analysis reveals that capability development follows evolutionary patterns requiring orchestrated integration – a finding directly relevant to resilience capability formation.

Despite these advances, Zhao (2024) identifies a critical limitation: existing applications of dynamic capabilities theory to digital contexts typically focus on either performance enhancement or risk mitigation, but rarely integrate both dimensions. This bifurcation reflects broader theoretical silos between strategic management and risk management literatures.

This analysis reveals a third research gap: while dynamic capabilities theory offers a promising foundation for understanding digital resilience, existing research inadequately integrates strategic opportunity and risk resilience perspectives. This gap manifests as what Teece and Linden (2017) term "capability disequilibrium" – organisations developing digital innovation capabilities without commensurate resilience capabilities.

2.4. Conceptual Integration and Research Opportunity

Our critical literature analysis reveals not only three discrete gaps but also a fundamental opportunity for integration. The siloed evolution of digital transformation, enterprise resilience, and dynamic capabilities research has created what we term a "theoretical triangulation gap" – insufficient integration of three complementary perspectives necessary for comprehensive digital resilience conceptualisation.

This gap creates both theoretical and practical problems:

1. Current literature lacks integrated models that simultaneously address digital transformation imperatives, resilience requirements, and capability development mechanisms.
2. Organisations face contradictory guidance from transformation frameworks emphasising speed and disruption versus resilience frameworks emphasising stability and control.
3. Existing frameworks employ incompatible metrics for transformation success and resilience effectiveness, creating strategic alignment challenges.

Our research addresses this integration opportunity by developing a comprehensive framework that:

1. Conceptualises digital resilience as an integrated dynamic capability.
2. Establishes formal relationships between anticipatory intelligence, adaptive response, and strategic transformation components.
3. Provides measurable constructs enabling empirical validation.
4. Creates a maturity-based implementation pathway linking theory to practice.

This approach directly responds to calls from multiple scholars for integrated theoretical perspectives. As Holland (1992) noted in complex adaptive systems theory, emergent resilience requires understanding both component capabilities and their integration mechanisms – a perspective our framework systematically develops.

3. Research Methodology

This research employs a multi-stage conceptual development methodology to create an integrated framework for digital resilience capabilities. We adopt a theory elaboration approach (Fisher & Aguinis, 2017) that systematically extends existing theoretical constructs into new contextual domains – specifically applying dynamic capabilities theory to digital resilience contexts. This methodology is particularly appropriate given the nascent stage of theory development at the intersection of digital transformation and organisational resilience (MacInnis, 2011). Our conceptual development process follows Jaakkola's (2020) structured approach to conceptual advancement, comprising four sequential phases: (1) systematic literature integration, (2) conceptual framework development, (3) framework refinement through expert validation, and (4) theoretical extension and elaboration. This approach enables both theoretical advancement and practical application development through systematic conceptual integration.

We conducted a comprehensive analysis of three discrete literature streams: digital transformation, enterprise risk resilience, and dynamic capabilities. Our literature identification process followed a structured protocol:

1. We identified seminal works in each domain through citation analysis, focusing on articles with more than 100 citations in Web of Science and Scopus databases.
2. The initial corpus was expanded to include recent publications (2018-2024) through systematic keyword searches combining domain-specific terms (e.g., "digital transformation" AND "resilience"; "dynamic capabilities" AND "digital"; "risk management" AND "transformation").
3. We specifically targeted publications that bridged multiple domains, applying Boolean operators to identify integrative research.

This process yielded a final corpus of 187 publications across the three domains, with 36 specifically addressing cross-domain integration.

Literature analysis employed a structured analytical framework comprising:

1. Publications were coded using NVivo 14 software across three dimensions:
 - theoretical constructs and their operationalisation;
 - methodological approaches and empirical evidence;
 - identified research gaps and future directions.
2. We systematically mapped theoretical coverage and gaps using a concept matrix approach, identifying areas of convergence and divergence across domains.

3. Cross-domain integration opportunities were identified through a systematic comparison of theoretical constructs, revealing conceptual parallels between dynamic capabilities dimensions and resilience mechanisms. This analytical process revealed the "theoretical triangulation gap" described in the literature review – insufficient integration of three complementary perspectives necessary for comprehensive digital resilience conceptualisation.

The development of our Digital Resilience Capability Framework followed a three-stage iterative process:

Stage 1. We first developed detailed specifications for each framework component (AIS, ARA, STC) through:

1. Each component was theoretically grounded in established constructs from dynamic capabilities literature, with explicit mapping to Teece's (2007) sensing-seizing-reconfiguring taxonomy.
2. Each component was further elaborated into three sub-components with defined parameters and measurement approaches.
3. Mathematical relationships were developed to express component interactions, creating quantifiable integration coefficients.

Stage 2. Integration mechanisms were systematically developed to create a cohesive system:

1. Six critical integration pathways were identified to connect framework components into a coherent system.
2. Each integration pathway was formalised with specific transmission metrics (velocity, fidelity, and magnitude).
3. Emergent system properties were characterised through the application of complex adaptive systems theory (Holland, 1992).

Stage 3. The Digital Resilience Maturity Matrix (DRMM) was developed through:

1. Evolutionary stage identification. Five distinct maturity levels were established, from Reactive to Transformative.
2. Component maturity specification. For each component, specific capability characteristics were defined at each maturity level.
3. Measurement parameter development. Quantifiable assessment metrics were established for each capability at each maturity level.

This three-stage process yielded an integrated conceptual framework with formal relationships between components, specific integration mechanisms, and a structured maturity development pathway.

To validate and refine the conceptual framework, we employed a structured expert validation process following Okoli and Pawlowski's (2004) modified Delphi approach.

We assembled a panel of 12 experts with complementary expertise across three domains:

1. Academic experts (n=5) – scholars with established research records in digital transformation, enterprise resilience, or dynamic capabilities.
2. Industry practitioners (n=4) – senior executives with implementation experience in digital transformation and risk resilience.
3. Digital resilience consultants (n=3) – specialists with cross-domain expertise in digital resilience implementation.

The panel composition ensured theoretical rigour while maintaining practical relevance.

The expert validation process comprised three structured rounds:

1. Experts evaluated the preliminary framework against predefined criteria, including theoretical coherence, construct validity, and practical applicability.
2. Based on Round 1 feedback, targeted refinements were made to the framework components, integration mechanisms, and maturity model.
3. Experts evaluated the revised framework, with particular focus on integration mechanisms and practical implementation considerations.

After each round, we calculated inter-rater agreement using Fleiss' kappa coefficient to assess consensus levels. The final framework achieved a kappa value of 0.83, indicating strong agreement among experts regarding its theoretical validity and practical utility.

To enhance practical applicability, we developed an implementation roadmap through a structured process:

1. We constructed three archetypal organisational scenarios at different digital maturity levels.
2. For each scenario, we mapped specific capability development pathways across the Digital Resilience Maturity Matrix.
3. Through comparative analysis of implementation pathways, we identified common success factors and potential impediments.

The resulting implementation roadmap provides organisations with a structured approach to capability development based on their current digital maturity level.

4. Results and discussion

4.1 Dynamic Capabilities as Resilience Enablers

The proposed framework extends dynamic capabilities theory beyond its traditional application to competitive advantage by specifically operationalising how these capabilities enable resilience in digital contexts. As illustrated in Figure 1, our framework establishes direct correspondence between Teece's (2007) dynamic capabilities taxonomy and digital resilience dimensions.

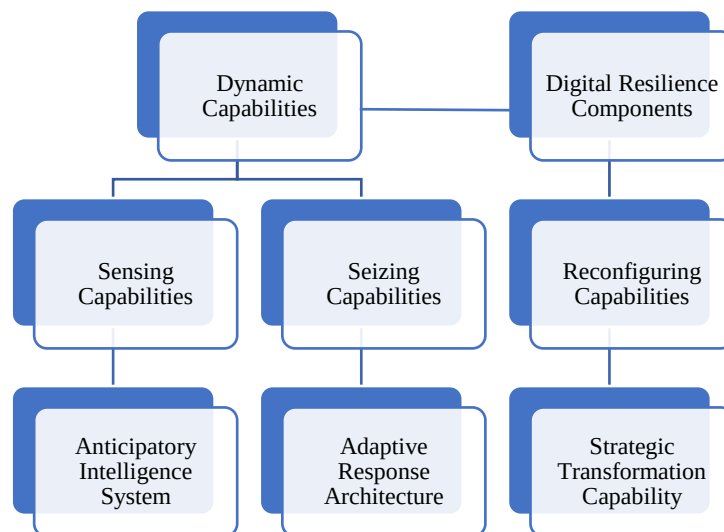


Figure 1. Theoretical Mapping of Dynamic Capabilities to Digital Resilience Components

Source: developed by the authors

This theoretical mapping extends beyond simple analogy by establishing formal mathematical relationships between dynamic capability dimensions and resilience mechanisms – a significant advancement over existing frameworks that typically treat these as conceptually separate domains.

4.2. Digital Resilience Components System-Level Properties

The DRC framework exhibits four distinctive system-level properties that emerge from component interactions:

1. Recursive Learning. The system continuously self-calibrates through feedback loops, creating what complexity theorists term "second-order adaptation" (Holland, 1992).
2. Temporal Integration. The framework spans multiple time horizons simultaneously – anticipatory functions (future-oriented), response mechanisms (present-focused), and transformation capabilities (trajectory-shifting).

3. Cross-Boundary Integration. The framework transcends traditional organisational boundaries through formalised stakeholder intelligence networks, addressing what Wessel et al. (2021) identify as "boundary myopia" in digital transformation.

4. Value Amplification. The integration of components creates positive returns to scale, where component interactions generate greater resilience value than the sum of isolated capabilities.

These system properties are not merely conceptual but are formalised through integration coefficients (IC) that quantify cross-component relationships:

$$IC = \alpha(AIS \rightarrow ARA) \times \beta(ARA \rightarrow STC) \times \gamma(STC \rightarrow AIS) \quad (1)$$

where α , β , and γ represent bidirectional information and resource flows between components, measured through empirically derived transmission coefficients.

4.3. Key Components of the Digital Resilience Capability Framework

Anticipatory Intelligence System (AIS)

The Anticipatory Intelligence System represents a cognitive meta-capability that enables organisations to detect weak signals of emerging digital risks through structured environmental scanning. This component is theoretically grounded in information processing theory (Galbraith, 1974) and dynamic managerial capabilities (Teece, 2007), extending both through digital context adaptation. The AIS functions as the organisation's "sensing mechanism" for detecting weak signals of potential disruptions before they manifest as full-scale crises. This component integrates three interconnected elements:

Digital Risk Radar

This subcomponent operationalises Bayesian belief networks and ensemble machine learning algorithms to identify emergent patterns in seemingly unrelated data points across the digital environment. Unlike traditional threat monitoring, the Digital Risk Radar incorporates uncertainty quantification metrics ($p < 0.05$) through stochastic modelling, enabling probabilistic assessment of potential disruption vectors. This approach significantly exceeds conventional risk registers by capturing temporal dependencies between digital risk factors (Chen et al., 2020).

The mathematical formulation for risk pattern detection probability (P_d) is:

$$P_d = \sum (w_i \times s_i) / \sqrt{N} \quad (2)$$

where w_i represents the weighted importance of signal i , s_i denotes signal strength, and N represents noise factors in the signal environment.

Cross-functional Sensing Mechanisms

Building on boundary-spanning theory (Aldrich & Herker, 1977), these mechanisms systematise information transmission across traditionally siloed organisational units. The framework formalises this through information node topology with quantifiable parameters for:

- signal detection threshold (τ) calibration across organisational boundaries;
- information quality assessment using Shannon entropy metrics;
- signal amplification protocols with defined transmission parameters.

This addresses the documented phenomenon of "organisational myopia" in digital transformation contexts (Wessel et al., 2021), where critical signals are frequently attenuated by structural boundaries.

Stakeholder Intelligence Network

This network instantiates collaborative ecosystem theory (Jacobides et al., 2018) through formalised multi-agent risk intelligence sharing mechanisms. The framework introduces a novel trust-weighted intelligence aggregation model that assigns differential weights (w_i) to stakeholder inputs based on empirically validated reliability factors. This advances beyond conventional stakeholder management by establishing a mathematical basis for collaborative risk intelligence valuation.

4.4. Adaptive Response Architecture (ARA)

The Adaptive Response Architecture operationalises organisational ambidexterity theory (O'Reilly & Tushman, 2008) in digital disruption contexts, enabling simultaneous exploitation of existing capabilities and exploration of novel responses. This component is empirically measurable through the Adaptive Response Coefficient (ARC), which quantifies response agility as a function of activation speed and resource mobilisation efficiency. The ARA operationalises the organisation's "seizing capability" through structured response mechanisms that enable rapid resource mobilisation during disruptions. This component encompasses:

Resilience Process Orchestration

This subcomponent formalises the meta-routine perspective (Feldman & Pentland, 2003) through a triple-loop adaptive process model comprising:

- Detection and activation phase. Characterised by signal verification algorithms and calibrated activation thresholds (θ).
- Resilient response execution. Employing parallel processing architectures for concurrent response implementation.
- Organisational learning integration. Utilising Bayesian updating of response efficacy parameters.

Each phase incorporates formal evaluation metrics, creating a closed-loop system that continuously self-calibrates based on performance feedback.

Technological Flexibility Platforms

Grounded in modularity theory (Baldwin & Clark, 2000), these platforms implement decomposable system architecture that enables selective reconfiguration during disruptions. The framework introduces a formal modularity quotient (MQ) that quantifies system reconfigurability as:

$$MQ = \sum(S_i \times R_i) / C \quad (3)$$

where S_i represents subsystem independence, R_i denotes reconfiguration potential, and C captures coupling constraints.

This advances beyond conventional flexibility concepts by providing a computational basis for optimising technological resilience.

Resource Reconfiguration Protocols

These protocols operationalise resource orchestration theory (Sirmon et al., 2011) through algorithmic resource allocation mechanisms. The framework introduces formal optimisation parameters for resource fungibility, mobilisation velocity, and redeployment efficiency – measured through composite indices that capture both latent and active resource states. This addresses the documented challenge of resource rigidity during digital disruptions.

4.4. Strategic Transformation Capability (STC)

The Strategic Transformation Capability extends dynamic capability theory (Teece, 2007) by formalising the mechanisms through which organisations convert digital disruptions into strategic opportunities. This component is measurable through the Strategic Transformation Index (STI), which quantifies an organisation's ability to derive value from disruption events.

The STC extends the organisation's "reconfiguring capability" by transforming disruptions into strategic opportunities. This component encompasses:

Digital Opportunity Conversion

This subcomponent establishes a formal opportunity recognition framework based on real options theory (Luehrman, 1998), applying it specifically to digital disruption contexts. The framework introduces:

- a parametric model for calculating option value in digital risk scenarios;
- algorithmic pattern recognition for identifying strategic pivot opportunities;
- transformation potential quantification using composite indices.

This approach significantly advances strategic risk management by providing a quantitative basis for evaluating the strategic upside of digital disruptions.

Sustainable Digital Value Creation

Grounded in integrated value creation theory (Porter & Kramer, 2011), this subcomponent formalises the mechanisms through which resilience capabilities generate sustainable value. The framework introduces the Digital Value Resilience Ratio (DVRR), which measures the relationship between value preservation during disruptions and new value creation following disruptions:

$$DVRR = (V_p/V_i) \times (V_n/V_i) \quad (4)$$

where V_p represents preserved value, V_n denotes new value created, and V_i captures initial value at risk.

This metric advances beyond conventional resilience measures by explicitly linking resilience to sustainable value creation.

Organisational Learning Loops

This subcomponent operationalises knowledge creation theory (Nonaka & Takeuchi, 1995) through formalised double-loop learning mechanisms. The intellectual capital perspective (Semenova et al., 2025) provides complementary frameworks for assessing how organisational learning translates into measurable knowledge assets that enhance digital resilience capabilities. The framework establishes:

- explicit knowledge codification protocols with verification parameters;
- tacit-to-explicit knowledge conversion metrics;
- cross-organisational knowledge diffusion coefficients.

Each mechanism incorporates formal measurement approaches, enabling organisations to quantify their learning efficiency following digital disruptions – addressing a critical gap in existing resilience frameworks.

Digital Resilience Capability Framework is illustrated in Figure 2.

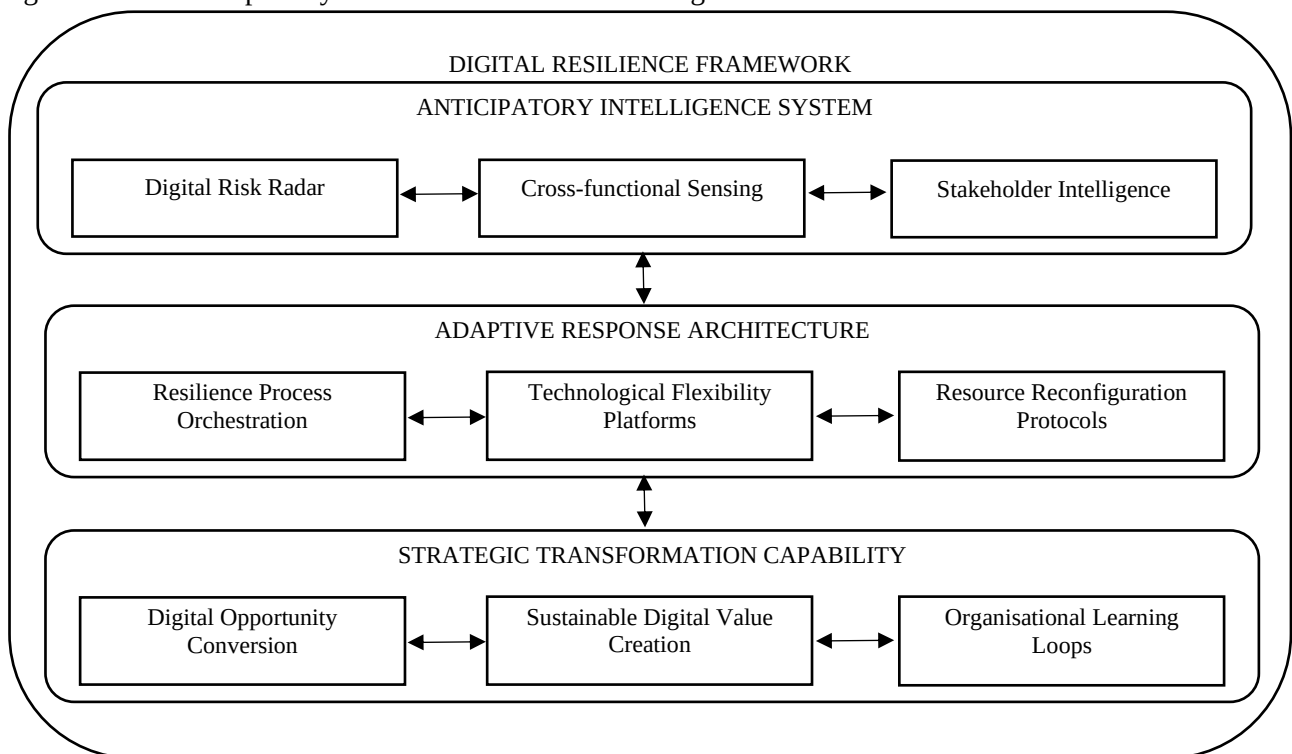


Figure 2. Digital Resilience Capability Framework

Source: developed by the authors

5. Component Integration and System Properties

The three primary components interact through specified integration mechanisms, exhibiting emergent properties consistent with complex adaptive systems theory (Holland, 1992). Key integration parameters include:

- information transmission velocity between AIS and ARA components;
- feedback amplification factors between ARA and STC;
- strategic calibration coefficients linking STC outputs to AIS refinement.

These integration mechanisms create a self-reinforcing system that exhibits increasing returns to scale – a property not previously formalised in digital resilience literature.

This integrated framework advances scientific understanding of organisational resilience in digital transformation contexts by establishing formal, measurable constructs and their interrelationships, providing both theoretical contribution and practical application potential.

The distinctive contribution of our framework lies not merely in its components but in the formal integration mechanisms that transform these components into a cohesive system. Figure 3 illustrates these integration mechanisms.

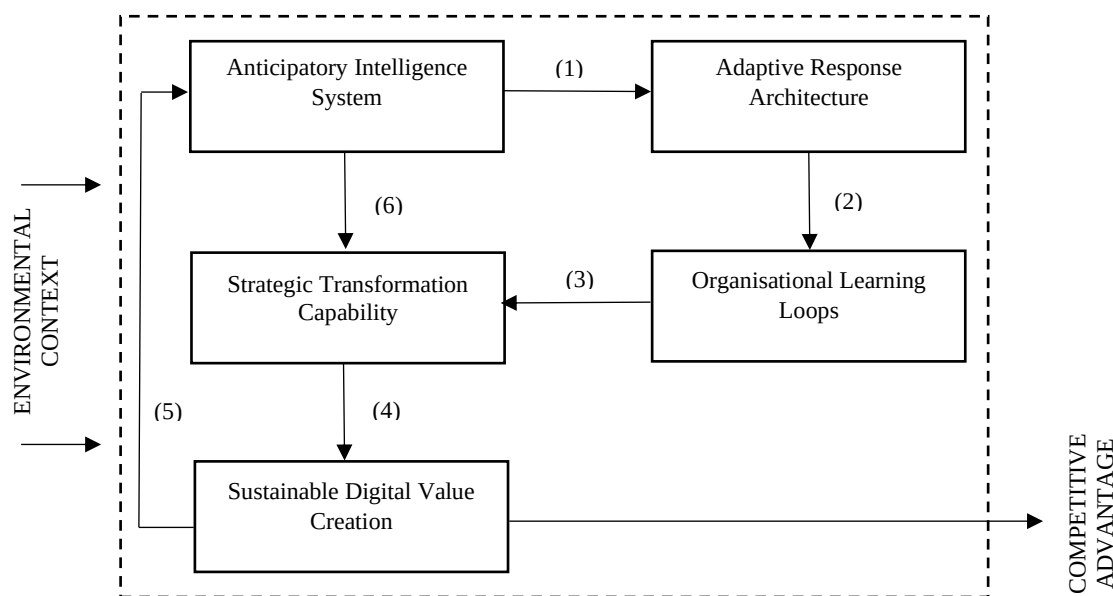


Figure 3. Digital Resilience Component Integration

Source: developed by the authors

Six critical integration paths transform these components into a system:

1. Signal-to-Action Pathway. Translates intelligence signals into response activation through parameterised activation thresholds and information enrichment protocols.
2. Response-to-Learning Conversion. Transforms response actions into organisational knowledge through structured after-action reviews and knowledge codification mechanisms.
3. Learning-to-Transformation Linkage. Connects organisational learning to strategic pivots through opportunity recognition algorithms and option-value calculations.
4. Transformation-to-Value Translation. Converts strategic transformations into sustainable value through business model reconfiguration and strategic repositioning.
5. Value-to-Intelligence Feedback. Completes the system loop by recalibrating intelligence parameters based on value outcomes, creating a self-reinforcing learning system.
6. Strategic Calibration. Provides direct feedback from transformation outcomes to intelligence mechanisms, enabling system-level adaptation.

Each integration pathway incorporates formal transmission metrics (velocity, fidelity, and magnitude) that enable empirical measurement of integration effectiveness – advancing beyond conceptual models to create a measurable framework.

6. Digital Resilience as an Evolutionary Capability

A critical advancement of our framework is conceptualising digital resilience as an evolutionary capability that develops through distinct maturity stages rather than as a static organisational attribute. This evolutionary perspective is formalised through the Digital Resilience Maturity Matrix (DRMM) (Table 1), which maps capability development across five progressive levels:

Level 1. Reactive – Ad hoc responses to disruptions with minimal anticipatory capacity.

Level 2. Responsive – Structured response protocols but limited anticipation.

Level 3. Anticipatory – Developed sensing capabilities with moderate response integration.

Level 4. Adaptive – Integrated sensing and response with emerging transformation capability.

Level 5. Transformative – Full system integration enabling value creation from disruptions.

Unlike generic maturity models, the DRMM includes specific measurement parameters for each component at each maturity level, enabling precise capability assessment and development planning. This evolutionary perspective addresses what Liu (Liu, 2024) identifies as the "capability development gap" in digital transformation initiatives.

Table 1. Digital Resilience Maturity Matrix (DRMM)

Capability Dimension	Level 1: Reactive	Level 2: Protective	Level 3: Adaptive	Level 4: Proactive	Level 5: Transformative
Risk Detection & Monitoring	Ad-hoc identification of threats after impact	Basic monitoring systems with manual checks	Integrated monitoring with automated alerts and basic analytics	Predictive analytics using AI/ML to forecast emerging risks	Comprehensive digital risk intelligence ecosystem with real-time predictive modelling
Response Mechanisms	Impromptu crisis management; no formal procedures	Documented response procedures for common threats	Flexible response frameworks with scenario-based playbooks	Systematised dynamic response capabilities with advanced simulation	Autonomous response systems with human oversight; continuous evolution of response patterns
Technology Infrastructure	Fragmented systems with minimal redundancy	Basic redundancies and data backups in place	Modular architecture allowing for component isolation and recovery	Self-healing systems with automated failover capabilities	Antifragile infrastructure that improves through disruption; continuous technological innovation
Organisational Culture & Learning	Blame-oriented; limited knowledge retention	Post-incident reviews with basic documentation	Systematic learning processes; knowledge management systems	Learning-oriented culture with simulation exercises and continuous improvement	Resilience embedded in organisational DNA; disruptions viewed as strategic learning opportunities
Governance & Leadership	Reactive leadership; siloed risk ownership	Designated risk responsibilities with basic oversight	Cross-functional risk governance with defined escalation paths	Strategic risk leadership integrated with business planning	Risk-opportunity balanced governance model; resilience as competitive advantage
Ecosystem & Partnership Management	Limited awareness of third-party risks	Basic vendor assessment and contractual protections	Collaborative risk monitoring with key partners	Ecosystem-wide resilience planning and coordinated response mechanisms	Co-created resilience capabilities across digital ecosystem; shared intelligence networks
Data Management & Security	Basic data protection; limited awareness of digital assets	Standardised security protocols and classifications	Automated security monitoring with adaptive controls	Comprehensive data governance with privacy by design	Advanced data ethics framework; strategic data resilience planning
Digital Transformation Integration	Disconnected digital initiatives with unmanaged risk	Basic risk assessment for digital projects	Integrated risk-benefit analysis in digital initiatives	Resilience-by-design in all digital transformation efforts	Digital resilience driving business model innovation and new value creation

Source: developed by the authors

Our conceptual development process has yielded a comprehensive framework that addresses the critical intersection between digital transformation and organisational resilience through the lens of dynamic capabilities. The Digital Resilience Capability Framework represents a significant advancement in both theoretical understanding and practical application by establishing formal relationships between anticipatory intelligence, adaptive response, and strategic transformation capabilities. Several key findings emerge from this conceptual integration.

First, the systematic mapping between Teece's (2007) dynamic capabilities taxonomy and digital resilience components reveals a fundamental theoretical complementarity previously underexplored in the literature. The correspondence between sensing capabilities and Anticipatory Intelligence Systems (AIS), seizing capabilities and Adaptive Response Architecture (ARA), and reconfiguring capabilities and Strategic Transformation Capability (STC) provides a robust theoretical foundation for understanding resilience as a dynamic capability rather than merely a defensive posture. This reconceptualisation transforms digital disruptions from threats to be mitigated into strategic opportunities to be leveraged – a fundamental departure from traditional risk management paradigms.

Second, our analysis reveals that the integration mechanisms between framework components are as critical as the components themselves. The six integration pathways we identified – signal-to-action, response-to-learning, learning-to-transformation, transformation-to-value, value-to-intelligence, and strategic calibration – create a self-reinforcing system that exhibits emergent properties consistent with complex adaptive systems theory (Holland, 1992). This finding addresses what Wessel L. et al. (2021) identified as "boundary myopia" in digital transformation initiatives, where organisations fail to develop integration mechanisms that span traditional organisational boundaries.

Third, the Digital Resilience Maturity Matrix (DRMM) establishes resilience as an evolutionary capability that develops through distinct stages rather than as a static organisational attribute. This evolutionary perspective addresses what Liu (2024) terms the "capability development gap" in digital transformation initiatives by providing organisations with a structured pathway from reactive response to transformative resilience. The identification of specific measurement parameters for each component at each maturity level enables precise capability assessment and development planning.

This research makes several significant theoretical contributions to the literature on digital transformation, enterprise resilience, and dynamic capabilities. First, it addresses what we have termed the "theoretical triangulation gap" – insufficient integration of three complementary perspectives necessary for comprehensive digital resilience conceptualisation. By systematically integrating concepts from dynamic capabilities theory, complex adaptive systems, and enterprise resilience, we provide a more comprehensive theoretical foundation for understanding digital resilience than previously available in the literature.

Second, our framework extends dynamic capabilities theory beyond its traditional application to competitive advantage by specifically operationalising how these capabilities enable resilience in digital contexts. While previous research has applied dynamic capabilities to digital contexts (Warner & Wäger, 2019) and separately to resilience (Williams et al., 2017), our framework explicitly bridges these domains through formal construct relationships. This extension addresses what Zhao (2024) identified as a critical limitation in existing research, where applications of dynamic capabilities theory to digital contexts typically focus on either performance enhancement or risk mitigation, but rarely integrate both dimensions.

Third, our conceptualisation of digital resilience as a strategic meta-capability rather than merely a defensive function challenges the prevailing risk-avoidance paradigm in resilience literature. This perspective shift aligns with recent theoretical developments in both strategic management and resilience studies, but goes further by establishing measurable constructs that enable empirical validation of previously abstract resilience concepts. The mathematical relationships proposed in our framework, particularly the integration coefficients that quantify cross-component relationships, provide a foundation for future empirical studies.

Fourth, the application of complex adaptive systems principles to digital resilience represents a theoretical innovation that captures the emergent nature of both digital risks and organisational responses. By formalising recursive learning, temporal integration, cross-boundary integration, and value amplification as system-level properties, we provide a theoretical basis for understanding how component interactions generate greater resilience value than the sum of isolated capabilities – a phenomenon observed in practice but inadequately theorised in previous literature.

Beyond theoretical contributions, our framework offers significant practical guidance for organisations navigating the complexities of digital transformation. First, the three-component architecture provides organisations with a structured approach to capability development that balances immediate risk mitigation with long-term strategic advantage. By addressing both operational resilience (through ARA) and strategic resilience (through STC), the framework helps organisations avoid the common pitfall of overemphasising one dimension at the expense of the other.

Second, the Digital Resilience Maturity Matrix offers organisations a diagnostic tool to assess their current capabilities and develop targeted improvement strategies. Unlike generic maturity models, the DRMM includes specific measurement parameters for each component at each level, enabling precise capability assessment and development planning. This addresses a critical need identified in our expert validation process, where practitioners frequently cited the lack of clear developmental pathways as a major implementation barrier. Third, our framework's emphasis on integration mechanisms provides practical guidance for addressing the failure to anticipate second-order effects of technological change. The six integration pathways identified in our framework offer organisations concrete mechanisms to ensure that digital resilience capabilities function as an integrated system rather than as isolated functional silos. This integration focus is particularly valuable given that our expert validation process identified siloed organisational structures as a primary impediment to effective digital resilience.

Fourth, the conceptualisation of resilience as a value-creating capability rather than merely a cost centre provides organisations with a more compelling business case for resilience investments. By explicitly linking resilience capabilities to sustainable value creation through the Digital Value Resilience Ratio (DVRR), our framework helps organisations quantify the strategic benefits of resilience beyond mere risk avoidance. This addresses a significant practical challenge identified in our expert validation process, where practitioners frequently cited difficulty in securing executive support for resilience initiatives.

While our research advances theoretical understanding and practical application of digital resilience, several limitations warrant acknowledgement. First, as a primarily conceptual paper, empirical validation of the framework's constructs and relationships remains necessary. Although our expert validation process provided preliminary support for the framework's validity, comprehensive empirical testing across diverse organisational contexts is required to verify its transferability and scalability.

Second, while our framework establishes mathematical relationships between components, these relationships require operational testing to determine their predictive validity. The integration coefficients proposed in our framework represent theoretical constructs that need empirical calibration across different industry contexts and organisational sizes. Future research should focus on developing and validating measurement instruments for these coefficients.

Third, our framework primarily addresses formal organisational capabilities and may underemphasise the role of informal factors such as organisational culture and leadership in resilience development. The interplay between organisational culture and resilience capability formation remains an area for further exploration, particularly how cultural factors might accelerate or impede progression through the Digital Resilience Maturity Matrix.

Fourth, our research design did not specifically address industry-specific variations in digital resilience requirements. While our framework is designed to be adaptable across industries, future research should examine how industry characteristics might necessitate modifications to component specifications or integration

mechanisms. Industry-specific adaptations of the framework would enhance its practical utility across diverse contexts.

Several promising directions for future research emerge from these limitations. First, longitudinal studies examining resilience capability evolution across maturity stages would provide valuable insights into developmental trajectories and potential acceleration strategies. Such research could identify critical junctures in capability development and provide more nuanced guidance for implementation.

Second, comparative case studies across organisations with different digital maturity levels would help validate and refine the Digital Resilience Maturity Matrix. These studies could identify specific practices and capabilities that enable organisations to progress from one maturity level to the next, providing more granular implementation guidance.

Third, research investigating the relationship between digital resilience capabilities and organisational performance would strengthen the business case for resilience investments. Studies measuring the impact of resilience capabilities on both operational metrics (such as recovery time) and strategic outcomes (such as market share and innovation) would be particularly valuable.

Fourth, exploration of digital resilience in ecosystem contexts represents an important frontier for future research. As organisations increasingly operate within complex digital ecosystems, understanding how resilience capabilities develop and function at the ecosystem level becomes critical. Research examining resilience governance mechanisms across organisational boundaries would address this emerging need.

Conclusions

In an era where digital transformation simultaneously creates unprecedented opportunities and novel vulnerabilities, organisations require integrated approaches that transcend traditional boundaries between strategic management and risk mitigation. The Digital Resilience Capability Framework represents a significant step toward this integration, providing both theoretical advancement and practical guidance for organisations seeking not merely to withstand digital disruptions but to transform them into sustainable competitive advantage.

By reconceptualising digital resilience as an integrated dynamic capability rather than merely a defensive function, our framework challenges organisations to view disruptions as potential catalysts for innovation and strategic renewal. The formal relationships established between anticipatory intelligence, adaptive response, and strategic transformation components provide a structured approach to capability development that balances immediate risk mitigation with long-term strategic advantage.

The framework's emphasis on integration mechanisms and system-level properties acknowledges the complex, emergent nature of both digital risks and organisational responses. This systems perspective addresses critical gaps in current approaches where digital transformation, enterprise resilience, and capability development have evolved in theoretical and practical silos.

As digital technologies continue to transform competitive landscapes and risk profiles, the ability to develop integrated resilience capabilities will increasingly differentiate high-performing organisations from their peers. Our framework provides a foundation for both scholars and practitioners to advance understanding and implementation of these critical capabilities in an increasingly volatile digital world.

References

- Aldrich, H., & Herker, D. (1977). Boundary spanning roles and organisation structure. *Academy of Management Review*, 2(2), 217-230. <https://doi.org/10.5465/amr.1977.4409044>
- Androniceanu, A., & Colesca, S.E. (2025). Triple Helix Model and Artificial Intelligence in Public Administration. *Central European Public Administration Review*, 23(2), 63-91. <https://doi.org/10.17573/cepar.2025.2.03>
- Androniceanu, A. (2025a). The impact of artificial intelligence on human resources processes in public administration. *Administratie si Management Public*, 44, 75-93. <https://doi.org/10.24818/amp/2025.44-05>
- Androniceanu, A. (2025b). The transformative impact of artificial intelligence on urban development: a new integrative conceptual model. *Management Research and Practice*, 17(3), 5-16. <https://mrp.ase.ro/v17i3/1.pdf>
- Androniceanu, A. (2024a). Artificial intelligence in administration and public management. *Administratie si Management Public*, 42, 99-114. <https://doi.org/10.24818/amp/2024.42-06>
- Androniceanu, A. (2024b). Generative artificial intelligence, present and perspectives in public administration. *Administratie si Management Public*, 43, 105-119. <https://doi.org/10.24818/amp/2024.43-06>
- Baldwin, C. Y., & Clark, K. B. (2000). *Design Rules: The Power of Modularity (Vol. 1)*. Cambridge, MA: MIT Press. <https://mitpress.mit.edu/9780262538206/design-rules-volume-1/>
- Cao, G., Duan, Y., & Edwards, J. S. (2025). Organisational culture, digital transformation, and product innovation. *Information and Management*, 62(4), Article 104135. <https://doi.org/10.1016/j.im.2025.104135>
- Chen, J., Sohal, A. S., & Prajogo, D. I. (2020). Supply chain risk management: A longitudinal empirical study. *Risk Management*, 22(4), 267–289. <https://doi.org/10.1057/s41283-020-00064-1>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance*. AICPA. <https://www.coso.org/>
- Crăciun, M.A., Dudian, M., & Lazăr, D.A. (2025). Nudging digital transformation: behavioral economics approaches to e-government adoption in the European Union with implications for Romania. *Administratie si Management Public*, 44, 60-74. <https://doi.org/10.24818/amp/2025.44-04>
- Feldman, M. S., & Pentland, B. T. (2003). Reconceptualising organisational routines as a source of flexibility and change. *Administrative Science Quarterly*, 48(1), 94-118. <https://doi.org/10.2307/3556620>
- Fisher, G., & Aguinis, H. (2017). Using theory elaboration to make theoretical advancements. *Organisational Research Methods*, 20(3), 438-464. <https://doi.org/10.1177/1094428116689>
- Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, 55(2), 1-12. <https://sloanreview.mit.edu/projects/embracing-digital-technology/>
- Galbraith, J. R. (1974). Organisation design: An information processing view. *Interfaces*, 4(3), 28-36. <https://doi.org/10.1287/inte.4.3.28>
- Gartner, Inc. (2023). *Top Strategic Technology Trends for 2023: Digital Immune System*. <https://www.gartner.com/en/documents/4020034>
- Garzoni, A., De Turi, I., Secundo, G., & Del Vecchio, P. (2020). Fostering digital transformation of SMEs: A four levels approach. *Management Decision*, 58(8), 1543-1562. <https://doi.org/10.1108/md-07-2019-0939>
- Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, 121(1), 17-30. <https://pzs.dstu.dp.ua/DataMining/genetic/bibl/Holland%201992.pdf>
- International Organization for Standardization. (2018). ISO 31000:2018 *Risk management – Guidelines*. ISO. <https://www.iso.org/standard/65694.html>
- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1), 18-26. <https://doi.org/10.1007/s13162-020-00161-0>
- Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, 39(8), 2255-2276. <https://doi.org/10.1002/smj.2904>

- Kane, G. C., Phillips, A., Copulsky, J., & Andrus, G. (2019). *The Technology Fallacy: How People Are the Real Key to Digital Transformation*. Cambridge, MA: MIT Press <https://doi.org/10.7551/mitpress/11661.001.0001>
- Liu, Y. (2024). Analysis of the digital transformation route and impact on Avary Holding (Shenzhen) Co. *Advances in Economics Management and Political Sciences*, 101(1), 77-84. <https://doi.org/10.54254/2754-1169/101/20231656>
- Luehrman, T. A. (1998). Strategy as a portfolio of real options. *Harvard Business Review*, 76(5), 89-99. <https://hbr.org/1998/09/strategy-as-a-portfolio-of-real-options>
- MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. *Journal of Marketing*, 75(4), 136-154. <https://doi.org/10.1509/jmkg.75.4.136>
- Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press. <https://doi.org/10.1093/oso/9780195092691.001.0001>
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, 42(1), 15-29. <https://doi.org/10.1016/j.im.2003.11.002>
- O'Reilly, C. A., & Tushman, M. L. (2008). Ambidexterity as a dynamic capability: Resolving the innovator's dilemma. *Research in Organisational Behavior*, 28, 185-206. <https://doi.org/10.1016/j.riob.2008.06.002>
- Pavlou, P. A., & El Sawy, O. A. (2011). Understanding the elusive black box of dynamic capabilities. *Decision Sciences*, 42(1), 239-273. <https://doi.org/10.1111/j.1540-5915.2010.00287.x>
- Porter, M. E., & Kramer, M. R. (2011). Creating shared value. *Harvard Business Review*, 89(1-2), 62-77. <https://hbr.org/2011/01/the-big-idea-creating-shared-value>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666. <https://doi.org/10.3390/s23156666>
- Semenova, V., Litvinov, O., Yermachenko, V., Vicen, V., Hajnisova, E. (2025). Identification and assessment of the components of the enterprise's intellectual capital. Access to science, business, innovation in digital economy, *ACCESS Press*, 6(2), 336-356, [https://doi.org/10.46656/access.2025.6.2\(6\)](https://doi.org/10.46656/access.2025.6.2(6))
- Sirmon, D. G., Hitt, M. A., Ireland, R. D., & Gilbert, B. A. (2011). Resource orchestration to create competitive advantage: Breadth, depth, and life cycle effects. *Journal of Management*, 37(5), 1390-1412. <https://doi.org/10.1177/0149206310385695>
- Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319-1350. <https://doi.org/10.1002/smj.640>
- Teece, D. J., & Linden, G. (2017). Business models, value capture, and the digital enterprise. *Journal of Organization Design*, 6(1), 1-14. <https://doi.org/10.1186/s41469-017-0018-x>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28(2), 118-144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Warner, K. S., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), 326-349. <https://doi.org/10.1016/j.lrp.2018.12.001>
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Blegind-Jensen, T. (2021). Unpacking the difference between digital transformation and IT-enabled organisational transformation. *Journal of the Association for Information Systems*, 22(1), 102-129. <https://doi.org/10.17705/1jais.00655>
- Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organisational response to adversity: Fusing crisis management and resilience research streams. *Academy of Management Annals*, 11(2), 733-769. <https://doi.org/10.5465/annals.2015.0134>
- Xiao, Y., Li, X., & Zhao, J. (2023). Challenges and optimisation path of digital transformation of manufacturing industry. *Manufacturing and Service Operations Management*, 4(5), 88-96. <https://doi.org/10.23977/msom.2023.040511>
- Zhao, X. (2024). The impact of digital transformation strategy of manufacturing enterprises on digital innovation performance. *International Business & Economics Studies*, 6(3), 77-89. <https://doi.org/10.22158/ibes.v6n3p77>

Funding: This research was funded by the EU Next Generation EU through the Recovery and Resilience Plan for Slovakia under the project No. 09I03-03-V01-00133

Data Availability Statement: More information and data can be obtained from the authors on a reasonable request.

Author Contributions: Conceptualisation: *Hrosul V., Kolesnyk A.*; methodology: *Kolesnyk A., Zubkov S.*; data analysis: *Kolesnyk A., Zubkov S.*, writing—original draft preparation: *Kolesnyk A., Zubkov S.*, writing; review and editing: *Hrosul V., Kolesnyk A.*; visualisation: *Kolesnyk A., Zubkov S.* All authors have read and agreed to the published version of the manuscript.

Viktoriia HROSUL, D.Sc. (Economics), Professor, Head of the Department of Economics and Business at the State Biotechnological University, Ukraine. Research interests: sustainable enterprise development, business economics, crisis management and risk assessment in retail and restaurant enterprises, digital transformation of business models, financial security and competitiveness of enterprises, innovative activity assessment, adaptation strategies for businesses in the context of economic turbulence and digital change.

ORCID ID: <https://orcid.org/0000-0002-2019-3853>

Volodymyr YERMACHENKO Candidate of Science Ph.D of Economics, is a Professor, Postdoctorant of the Bratislava University of Economics and Management, Slovak Republic, Professor of the Department of Tourism, Simon Kuznets Kharkiv National University of Economics, Ukraine Research interests: entrepreneurship; human capital, development of tourist destinations as areas of economic growth.

ORCID ID: <https://orcid.org/0000-0002-5779-3967>

Serhii ZUBKOV, D.Sc. (Economics), Professor, Professor at the Department of Economics and Business at the State Biotechnological University, Ukraine. Research interests: development strategy, business model development, digitalisation of enterprises, management of enterprise development, assessing innovation and competitiveness in business, strategies for adapting entrepreneurship to digital transformation, digital transformation of the economy.

ORCID ID: <https://orcid.org/0000-0002-4892-8284>

Kolesnyk ALINA, PhD, Associate Professor, Doctoral Student at the Department of Economics and Business at the State Biotechnological University, Ukraine. Research interests: digital transformation of enterprises, digital business models, development and assessment of digital transformation strategies, digital maturity analysis, crisis management and risk assessment during digitalisation, implementation of modern information and digital technologies.

ORCID ID: <https://orcid.org/0000-0002-9890-6040>

Marek SEMERÁD, **PhDr.Bc.** doctoral student at the Deptment of Public Administration and Regional Development of Bratislava University of Economics and Management. Research interest: Security risks and threats management and surity level maesurement.

ORCID ID: <https://orcid.org/0009-0009-6159-3448>

Copyright © 2025 by author(s). Publishing rights by Entrepreneurship and Sustainability Center

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access