УДК 005.334:005.21:004.9
DOI: https://doi.org/10.30838/EP.214.335-343

Reznikov Roman
PhD in Economic Sc.
Institute of Industrial Economics of the NAS of Ukraine
Резніков Р.Б.
доктор філософії з економіки
Інститут економіки промисловості НАН України
https://orcid.org/0000-0001-5581-5651

THE RR-FRAMEWORK 3.0: AN OPEN SPREADSHEET-BASED MODEL FOR INTEGRATED ASSESSMENT OF BUSINESS RESILIENCE, DIGITAL MATURITY AND CRISIS-DRIVEN STRATEGY PRIORITIZATION

The article substantiates the RR-framework 3.0, an open spreadsheet-based model for integrated assessment of business resilience, digital maturity and crisis-driven strategy prioritization. The relevance of the study is defined by compound disruptions and by the lack of affordable diagnostic tools for small and medium-sized organizations. The model links self-assessment with confidence-adjusted maturity scoring, industry gaps, applicability gates, a risk engine, crisis-scenario adjustment, fuzzy resilience posture, WSJF prioritization and analytic plus Monte Carlo-based index approximation of tail-risk exposure. A synthetic fintech case under a severe cyber/ransomware scenario demonstrates domain diagnostics, exposure ranking, tail-exposure estimates and a wave-based roadmap. The practical value lies in a transparent and reproducible instrument that connects diagnostics with managerial action.

***Keywords**: business resilience, digital maturity, crisis management, semi-quantitative risk assessment, fuzzy logic, WSJF prioritization, VaR/CVaR-like tail-exposure index, strategy roadmap, maturity model, organizational resilience.*

***JEL classification:** M15, O33, D81, G32, L25.*

RR-FRAMEWORK 3.0: ВІДКРИТА ТАБЛИЧНА МОДЕЛЬ ІНТЕГРОВАНОГО ОЦІНЮВАННЯ БІЗНЕС-СТІЙКОСТІ, ЦИФРОВОЇ ЗРІЛОСТІ ТА ПРІОРИТИЗАЦІЇ АНТИКРИЗОВОЇ СТРАТЕГІЇ

Статтю присвячено обґрунтуванню та опису RR-framework 3.0 - відкритої табличної моделі, що інтегрує оцінювання зрілості процесів, рівня цифровізації та організаційної стійкості бізнесу в єдиний аналітичний ланцюг і перетворює структуроване самооцінювання на кризову експозицію, пріоритизовані ризики, стратегічні пакети та готовий до виконання план дій. Актуальність теми зумовлена зростанням частоти складених, взаємопідсилюваних збурень - кібератак, збоїв ланцюгів постачання, регуляторних і геополітичних шоків, - а також стійким розривом між концепціями стійкості високого рівня та інструментами, які малі й середні організації здатні реально застосувати без залучення дорогого консалтингу. Метою дослідження є розроблення прозорого, відтворюваного та доступного інструменту інтегрованої діагностики стійкості й цифрової зрілості, який безпосередньо пов'язує результати оцінювання з керованими діями. Методологічну основу становлять системний підхід, моделі організаційної зрілості, теорія динамічних здатностей, нечітка логіка, методологія пріоритизації за зваженою вартістю затримки (WSJF), а також аналітичне й імітаційне (Монте-Карло) індексне наближення хвостової ризикової експозиції з VaR/CVaR-подібними показниками. Модель побудовано на шкалі зрілості 0–5 із коригуванням на достовірність свідчень і впевненість оцінювача, на галузевих цільових розривах, фільтрах релевантності та застосовності, містку здатностей, рушії ризиків зі специфічними для рівня заходами реагування, шарі кризових сценаріїв, нечіткому профілі стійкості та пріоритизації ініціатив із формуванням хвиль дорожньої карти. Практичну апробацію наведено на синтетичному прикладі платіжної фінтех-компанії в умовах важкого сценарію кібератаки з програмою-вимагачем: робоча книга формує доменну діагностику, рейтинг експозиції, умовні індексні оцінки очікуваних втрат і пріоритизований, розподілений за хвилями план дій. Практична цінність одержаних результатів полягає у наданні бізнесу, консультантам і дослідникам відкритого, безкоштовного та методологічно узгодженого засобу, що поєднує діагностику стійкості з конкретними рішеннями й підвищує обґрунтованість антикризового управління та цифрової трансформації підприємства.

***Ключові слова:** бізнес-стійкість, цифрова зрілість, антикризове управління, напівкількісне оцінювання ризиків, нечітка логіка, пріоритизація WSJF, VaR/CVaR-подібний індекс хвостової ризикової експозиції, стратегічна дорожня карта, модель зрілості, організаційна стійкість.*

ISSN друкованої версії: 2224-6282
ISSN електронної версії: 2224-6290

Formulation of the problem. The contemporary operating environment of business organizations is shaped by disruptions that are increasingly frequent, interconnected and difficult to forecast. Cyberattacks and ransomware, breakdowns in global supply chains, energy and inflation shocks, abrupt regulatory change, pandemics and armed conflict no longer occur as isolated, low-probability events but as overlapping pressures that propagate across functions and amplify one another. The World Economic Forum consistently ranks technological, societal and geopolitical risks among the most severe threats to organizations over both the short and the long term [1, p. 7–18]. In such conditions the ability of a company not merely to survive a single shock, but to absorb, recover from and adapt to a continuous stream of disruptions, becomes a strategic determinant of competitiveness and long-term value.

Two managerial capabilities have become central to this agenda. The first is organizational resilience - the capacity to anticipate, withstand, recover and reconfigure in the face of adversity [2, p. 47–61; 3, p. 1–318]. The second is digital maturity - the degree to which an organization has integrated digital technologies, data and automation into its processes and decision-making, which strongly conditions its capacity to sense and respond to disruption [4, p. 1–292; 5, p. 1–31]. International standards such as ISO 22301 on business continuity management [6, p. 1–28] and ISO 31000 on risk management [7, p. 1–16] codify the principles of these disciplines, yet they remain deliberately generic and provide requirements rather than a ready computational instrument that a particular organization can pick up and run.

Herein lies the practical problem. There is a persistent gap between, on the one hand, an abundant conceptual and normative literature on resilience, maturity and risk, and, on the other, the scarcity of transparent, affordable and reproducible tools that translate these concepts into concrete diagnostics and actions for a specific firm. Large corporations can commission bespoke consulting engagements; small and medium-sized enterprises (SMEs), which form the backbone of most economies, usually cannot. They need an instrument that is comprehensive enough to cover the whole organization, rigorous enough to be defensible, and simple enough to be operated without proprietary platforms or specialized data-science teams. Addressing this gap - by designing an open, integrated and executable assessment model - is the problem to which this article is devoted.

Analysis of recent research and publications and the unresolved part of the problem. The scholarly foundation of the present study is structured along four interrelated streams. The first concerns the conceptualization and measurement of organizational and system resilience. Hosseini, Barker and Ramirez-Marquez systematized the proliferating definitions and quantitative measures of resilience and showed that the field still lacks a unified, operational metric [2, p. 47-61]. Annarelli and Nonino linked the strategic and operational dimensions of resilience management [8, p. 1–18], while Duchek advanced a capability-based conceptualization that frames resilience as a dynamic, stage-wise process of anticipation, coping and adaptation [9, p. 215–246]. Linkov and co-authors argued for a shift from narrow risk analysis to a resilience paradigm built around system functions [10, p. 407-409], and Sheffi demonstrated how investments in flexibility and redundancy convert disruption into competitive advantage [3, p. 1–318].

The second stream addresses maturity modeling as an assessment paradigm. Since the Capability Maturity Model formalized staged improvement of organizational processes [11, p. 18-27], maturity models have become a widely used genre for diagnosing the as-is state of a capability and charting a path to a target level. Becker, Knackstedt and Poeppelbuss formulated design requirements for rigorous, procedurally sound maturity models, cautioning against ad-hoc constructs that lack methodological transparency [12, p. 213-222]. This stream supplies the 0–5 staged-scale logic that underlies maturity scoring.

The third stream concerns digital transformation and dynamic capabilities. Westerman, Bonnet and McAfee established the empirical link between digital maturity and superior firm performance [4, p. 1–292], and the longitudinal MIT–Deloitte research programme of Kane and colleagues identified strategy, culture and talent - rather than technology alone — as the principal drivers of digital maturity [5, p. 1–31]. Teece's theory of dynamic capabilities provides the strategic-management foundation for understanding how firms reconfigure resources under change [13, p. 509–533]. The author's own prior work extends this stream to the microeconomic impact of cloud technologies and Industry 4.0 [14, p. 67–74], to the strategic adoption of generative artificial intelligence in enterprises [15, p. 1–7], and to the typology and management of crises in technology-intensive companies [16, p. 1–5; 17, p. 95–100].

The fourth stream supplies the quantitative apparatus for prioritization and risk. Reinertsen's principles of product-development flow introduced the Weighted Shortest Job First (WSJF) logic and the notion of cost of delay, which has since become a standard for economic sequencing of initiatives [18, p. 1–294]. Zadeh's theory of fuzzy sets enables the representation of graded, linguistic states such as fragile, exposed or resilient without forcing artificial binary cut-offs [19, p. 338–353]. Artzner and co-authors defined coherent measures of risk and the properties a sound risk metric must satisfy [20, p. 203–228], and Rockafellar and Uryasev developed the optimization of conditional value-at-risk (CVaR), the tail-risk measure used to characterize severe-loss exposure [21, p. 21–41].

Summarizing these streams reveals that, despite a rich body of work, resilience, digital maturity, semi-quantitative risk-exposure estimation and initiative prioritization are predominantly studied as separate objects, each with its own instruments and vocabulary. Maturity models rarely connect their scores to crisis exposure; resilience frameworks seldom terminate in an economically sequenced, executable roadmap; and VaR/CVaR-inspired tail-risk indicators are rarely embedded inside an accessible self-assessment that a non-specialist can run. The unresolved part of the general problem, therefore, is the absence of a single, open and reproducible model that integrates maturity, digitalization and resilience assessment with crisis-scenario adjustment, semi-quantitative risk-exposure estimation and WSJF-based roadmap prioritization within one transparent computational artifact. It is precisely this integration gap that the RR-framework 3.0 is designed to close.

The aim and objectives of the article. The aim of the article is to present and substantiate the RR-framework 3.0 as an open, spreadsheet-based model for the integrated assessment of business resilience, digital maturity and crisis-

driven strategy prioritization, and to demonstrate its logic, mechanics, content and practical value on a worked example.

To achieve this aim, the following research objectives are set: (1) to formulate the conceptual logic of the model and its end-to-end assessment chain; (2) to describe the architecture, content and scoring mechanics of the workbook, including confidence adjustment, gap analysis, the risk engine, the crisis and fuzzy-posture layers, and WSJF prioritization; (3) to show how the model quantifies crisis exposure and tail risk through analytic and Monte Carlo estimation; (4) to illustrate the model outputs on a demonstration case and to characterize the practical value, limitations and prospects of the instrument.

Research methods. The study applies a combination of general scientific and special methods. The systems approach is used to treat the organization as a multi-level structure of interacting domains, so that resilience emerges from the configuration of process maturity, digitalization and control across the whole enterprise rather than from any single function. Methods of analysis and synthesis, abstraction and generalization underpin the design of the assessment model and the consolidation of heterogeneous evidence into composite indicators. The maturity-model method provides the staged 0–5 scale and the gap-analysis logic. The WSJF method of weighted cost of delay is used for the economic prioritization of initiatives. Methods of semi-quantitative probabilistic risk analysis - analytic Normal expected-shortfall estimation and seeded Monte Carlo simulation - are applied to approximate index-based loss distributions and VaR/CVaR-like tail-exposure indicators. The model is implemented as a macro-free Microsoft Excel workbook, which guarantees transparency, auditability and reproducibility of every calculation. The instrument is validated through structured synthetic test cases; results are illustrated on one such case throughout the article.

Presentation of the main research results. *The conceptual logic and the assessment chain.* The RR-framework 3.0 is built around a single idea: a structured self-assessment of an organization should not end with a score, but should flow, by transparent rules, all the way to a prioritized plan of action that accounts for the specific crisis the organization fears most. The model therefore implements a canonical, one-directional chain. A company profile defines context and is compressed into a profile vector (industry, scale, business and operating model). This vector calibrates the assessment of 424 questions organized into 17 business domains and 76 subdomains. Raw answers pass through relevance and applicability gates and through evidence and assessor confidence adjustment; a capability bridge connects domain scores to a risk engine that draws on a library of 424 risk rows with 2,544 score-specific risk statements and 2,544 score-specific treatments. A crisis engine and a fuzzy posture layer adjust exposure for the selected scenario; a strategy engine selects from 14 strategy packages; and an initiatives engine ranks 72 initiatives by WSJF and distributes them across roadmap waves. The chain terminates in visible dashboards [22] (Fig. 1).

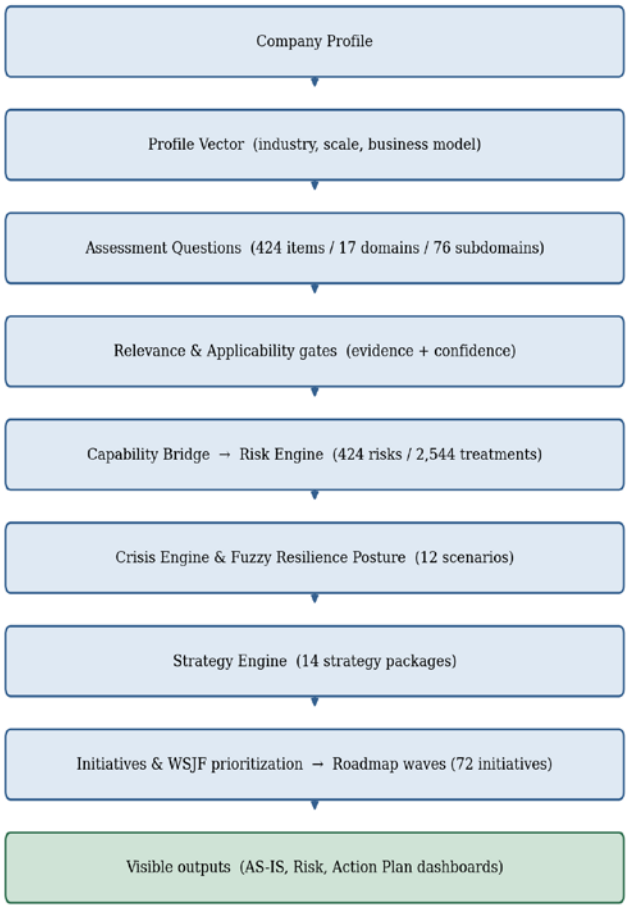

Fig. 1. The canonical assessment chain of the RR-framework 3.0.
Source: created by Author.

Architecture and content. The workbook is engineered as a 43-sheet model - six visible workflow sheets and 37 hidden layers for data, engines, configuration, reference libraries and an internal documentation and audit layer. The visible workflow guides the user through Guidelines, Company Profile, Assessment Questions, AS-IS Assessment, Resilience & Risk Scenario and Action Plan & Roadmap. Because the workbook contains no macros and stores all logic in cell formulas, every number is traceable to its inputs, which is essential for trust and for academic reproducibility. The scale of the model is summarized in Table 1.

Table 1

Architecture and content scale of the RR-framework 3.0

Indicator	Value
Workbook sheets (visible / hidden)	43 (6 / 37)
Formulas	90,275
Assessment questions	424
Business domains / subdomains	17 / 76
Score-specific risk statements	2,544
Score-specific treatment statements	2,544
Initiatives / strategies	72 / 14
Crisis scenarios	12
Industry templates / aliases	10 / 42
Monte Carlo iterations	2,000

Source: Created by Author.

Scoring mechanics. Each question is scored on a 0–5 maturity scale, where 0 denotes a non-existent or unevidenced capability and 5 denotes an optimized, integrated and continuously improved one. Domain scores are weighted aggregates of question scores; targets are industry-specific; and gaps drive priority. The weighted domain score is

$$Domain\ Score\ =\ \Sigma(Question_i\ \times\ Weight_i)\ /\ \Sigma(Weight_i) \quad (1)$$

To avoid overconfidence where evidence is weak, each score is multiplied by a confidence factor combining evidence and assessor confidence:

$$Confidence-Adjusted\ Score\ =\ Raw\ Score\ \times\ Evidence\ Factor\ \times\ Assessor\ Factor \quad (2)$$

Priorities are then derived from the distance to the industry target, weighted by an industry criticality multiplier, so that the same gap matters more in a domain that is critical for the sector:

$$Gap\ Priority\ =\ max(0,Target\ -\ Score)\ \times\ Criticality\ Multiplier \quad (3)$$

Maturity diagnostics on the demonstration case. The illustrative case is a synthetic fintech payments company (PayHarbor Financial Technologies; 420 employees; hybrid cloud; critical regulatory exposure) assessed against a Financial Services / Banking template. The overall confidence-adjusted maturity is 2.25 of 5, at the 47th industry percentile, with an average gap to target of 2.2 and thirteen red-line control breaches. Figure 2 contrasts the confidence-adjusted maturity of each domain with its industry target. The widest gaps appear in Cyber Privacy, IT Cloud & Disaster Recovery, Legal Risk, Governance & Crisis and Business Systems — exactly the domains a regulated payments firm cannot afford to leave immature.

Table 2 reports a diagnostic excerpt: for each domain the confidence-adjusted maturity, the industry target, the resulting gap and the threshold status. A status of Breach marks a domain that falls below the red-line floor and therefore demands immediate attention, whereas Gap marks a shortfall that is material but not critical.

Crisis adjustment and fuzzy resilience posture. The distinctive contribution of the model is that maturity is not assessed in the abstract but against a concrete crisis. The user selects a scenario and a severity from 1 to 5; the crisis engine then applies scenario-specific multipliers to each domain, so that the same weakness produces different exposure depending on the threat. For the demonstration case the active scenario is a cyberattack / ransomware event at maximum severity 5. Domain exposure is computed as a crisis-adjusted function of weakness and criticality, and the resulting ranking (Fig. 3, left) places Cyber Privacy, IT Cloud & DR and Data BI & AI at the top. In parallel, fuzzy-set logic [19, p. 338–353] maps the organization onto five graded resilience states. The demonstration case is dominated by the Exposed state (membership 0.80) with partial Adaptive membership (0.16) and zero Resilient membership (Fig. 3, right), and the model recommends a Business Continuity and Resilience posture as the leading strategic stance.

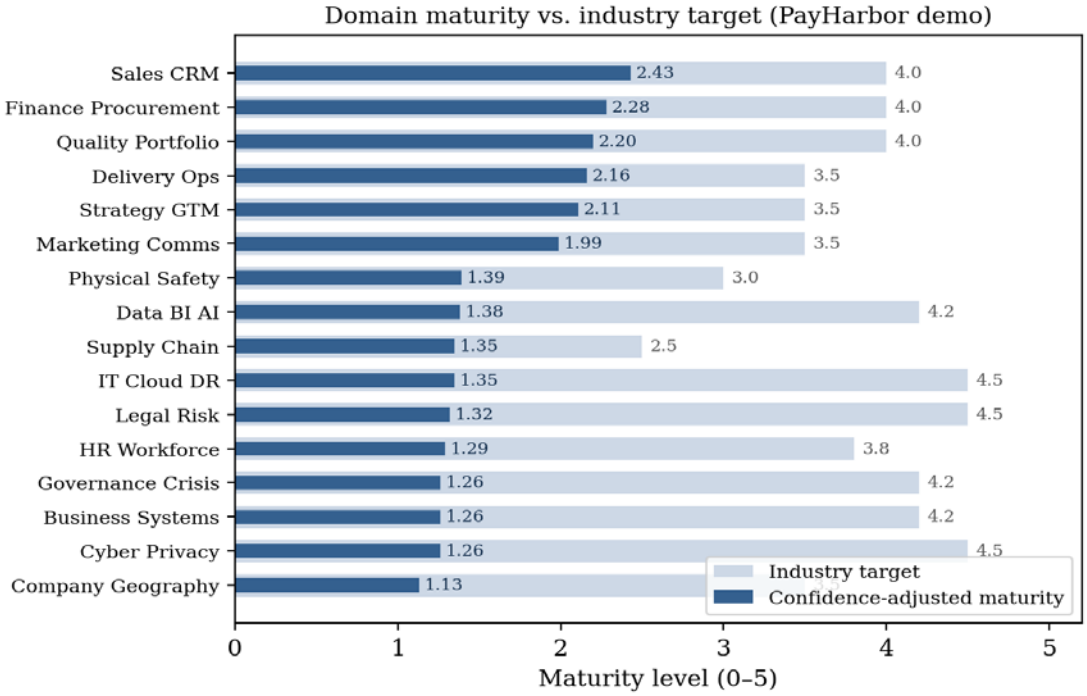

Fig. 2. Domain maturity versus industry target (demonstration case)
Source: created by Author.

Table 2

Domain diagnostics of the demonstration case (excerpt)

Domain	Maturity	Target	Gap	Status
Cyber Privacy	1.26	4.5	3.24	Breach
IT Cloud DR	1.35	4.5	3.15	Breach
Legal Risk	1.32	4.5	3.18	Breach
Governance Crisis	1.26	4.2	2.94	Breach
Business Systems	1.26	4.2	2.94	Breach
Data BI AI	1.38	4.2	2.82	Breach
Finance Procurement	2.28	4.0	1.72	Breach
Delivery Ops	2.16	3.5	1.34	Gap
Supply Chain	1.35	2.5	1.15	Gap

Source: created by Author.

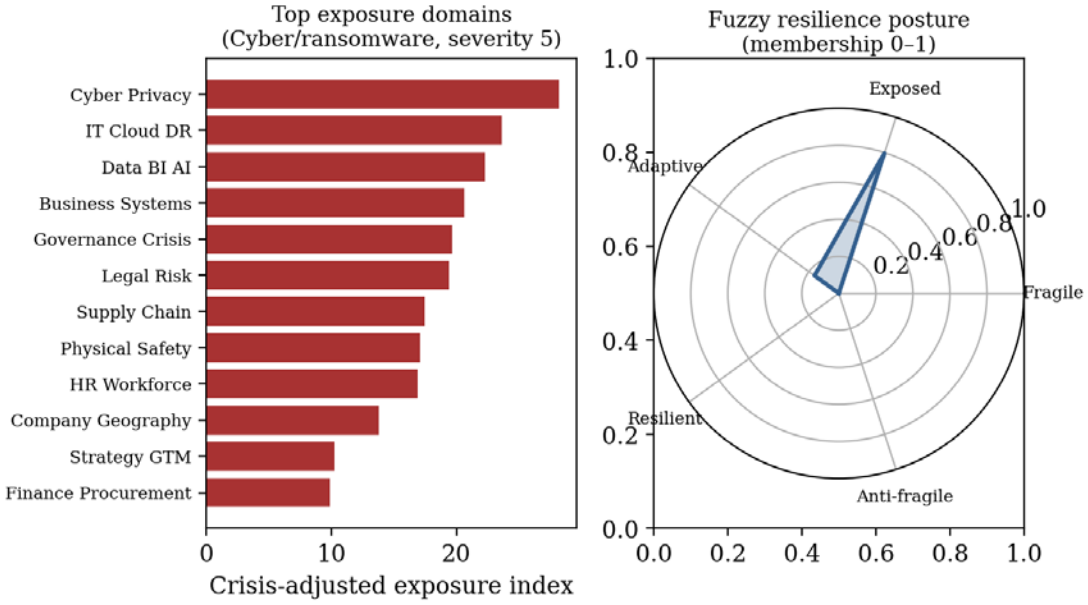

Fig. 3. Crisis-adjusted domain exposure and fuzzy resilience posture (cyber/ransomware, severity 5)
Source: created by Author.

Quantification of tail-risk exposure. To translate exposure into comparable index terms, rather than firm-specific actuarial loss amounts, the model estimates a resilience loss-index distribution and its tail indicators. Two complementary methods are used: an analytic Normal expected-shortfall model and a seeded, reproducible Monte Carlo simulation of 2,000 iterations with a systemic-shock component. The conditional value-at-risk-like indicator, which characterizes the expected severity of index losses beyond the value-at-risk-like threshold, is defined as:

$$CVaR\alpha = E[L \mid L \geq VaR\alpha] \quad (4)$$

For the demonstration case the analytic 95% VaR-like exposure index is 94.5 thousand index units and the 95% CVaR-like tail-exposure index is 101.6 thousand, while the seeded Monte Carlo model returns a 95% VaR-like exposure index of 97.5 thousand and a 99% VaR-like exposure index of 116.8 thousand (Fig. 4). The use of a frozen random seed makes the simulation fully reproducible, while the interpretation of these values remains explicitly index-based and semi-quantitative rather than actuarial [20, p. 203–228; 21, p. 21–41].

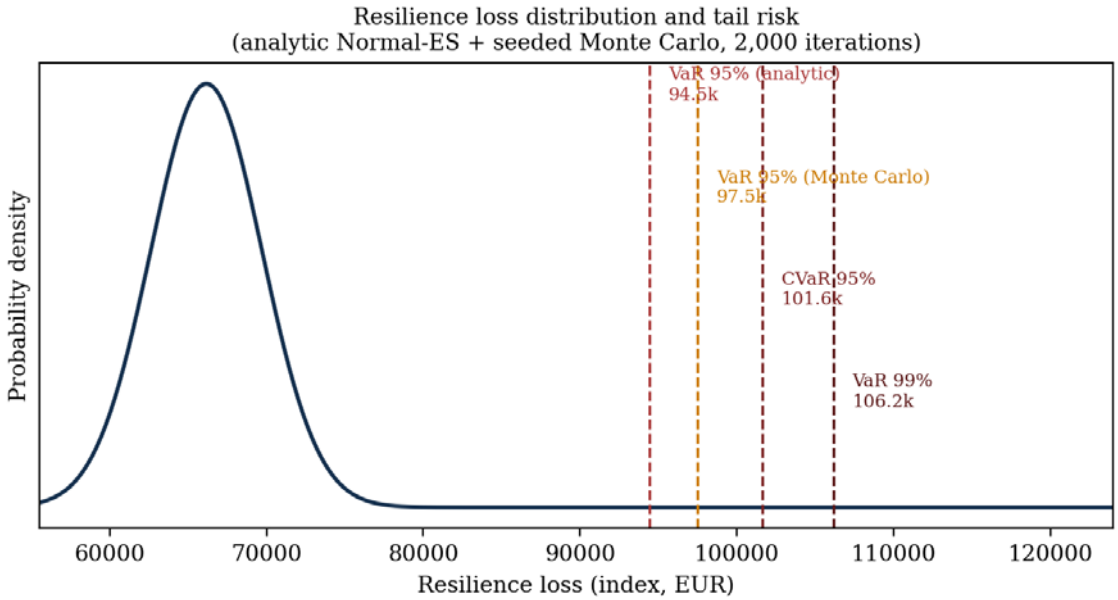

Fig. 4. Resilience loss-index distribution and VaR/CVaR-like tail-exposure measures (analytic and Monte Carlo)
Source: created by Author.

Strategy selection and WSJF roadmap. The final stage converts the diagnosis into action. The strategy engine selects a primary strategy package - for the demonstration case, a Cyber Resilience Strategy supported by a Cloud and Infrastructure Resilience Strategy - and the initiatives engine ranks 72 initiatives by the Weighted Shortest Job First score, computed as the aggregated cost of delay divided by the relative job size:

$$WSJF = (BV + TC + RR + OE) / JS \quad (5)$$

Initiatives are then distributed across roadmap waves (0–90 days, 3–6 months, 6–12 months, 12+ months). For the demonstration case the twelve highest-scoring initiatives - led by compliance obligation monitoring (WSJF 4.18), mapping of critical business dependencies (4.15) and data and intellectual-property safeguards (4.13) - are scheduled into the first 90-day wave, with a further eight initiatives in the 3–6 month wave (Fig. 5). Each initiative carries an estimated avoided loss, so that the roadmap is sequenced by economic value rather than by intuition. In this way the model closes the loop from a single questionnaire answer to a financially justified, time-phased action plan.

Value and positioning of the instrument. The integrated design yields several distinctive benefits. First, it unifies in one artifact capabilities that are usually dispersed across separate maturity, resilience and risk tools, eliminating the loss of information that occurs when scores, risks and plans live in disconnected documents. Second, it is transparent and reproducible: with no macros and a frozen simulation seed, every output can be audited and re-derived, which is rare among comparable commercial tools and important for scholarly use. Third, it is open and free under a Creative Commons licence and is published with a citable DOI and ORCID attribution [22], lowering the barrier for SMEs, consultants and researchers. Fourth, it is action-oriented: the WSJF roadmap and avoided-loss estimates make the assessment immediately decision-relevant. These properties position the RR-framework as a practical bridge between the conceptual resilience and maturity literature [2, p. 47–61; 3, p. 1–318; 4, p. 1–292; 5, p. 1–31; 8, p. 1–18; 9, p. 215–246; 10, p. 407–409; 11, p. 18–27; 12, p. 213–222; 13, p. 509–533] and the operational reality of organizations that must act under uncertainty. At the same time, the model has limitations that define its scope of valid use: it relies on the honesty and competence

of self-assessment; its industry templates and multipliers, though calibrated, are expert-based and benefit from further empirical validation; and the loss distribution is an index-based approximation rather than a firm-specific actuarial model. The model therefore should not be interpreted as a full actuarial or financial-statistical VaR/CVaR model based on long historical series of actual firm-specific losses. Instead, it uses an expert-calibrated, index-based approximation of VaR/CVaR-like indicators, which should be read as conditional indices of tail-risk exposure rather than statistically validated monetary estimates of expected losses. Its primary purpose is not precise forecasting of financial losses, but semi-quantitative risk ranking, comparison of crisis-impact scenarios and support for selecting priority managerial initiatives to improve enterprise resilience. These limitations are inherent to lightweight diagnostic instruments and outline the agenda for the model's continued development.

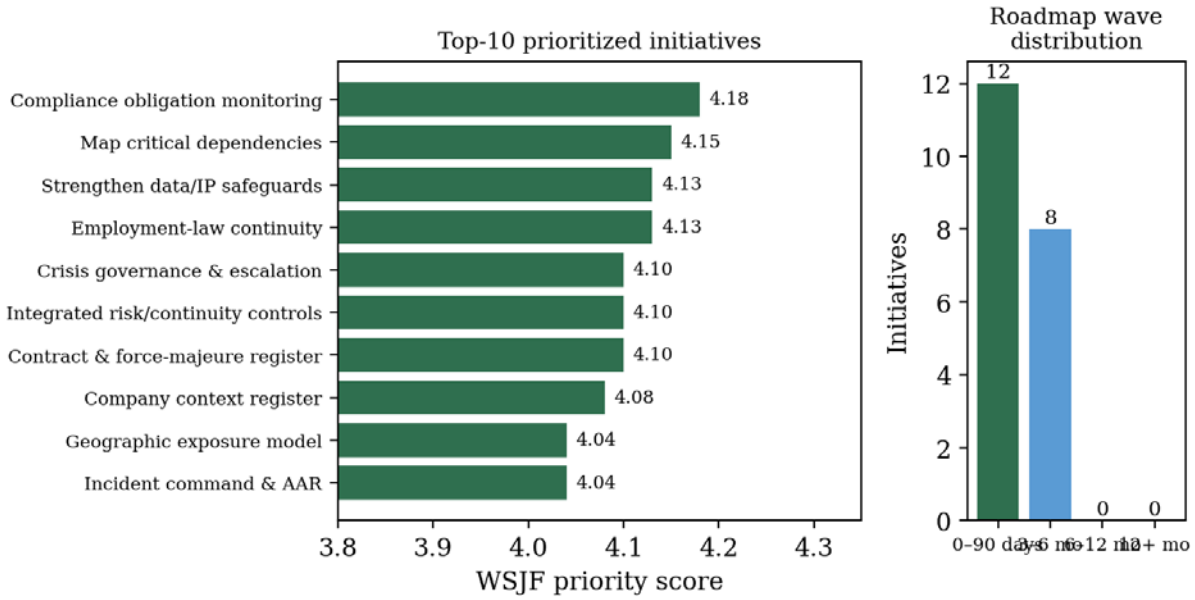

Fig. 5. Top prioritized initiatives by WSJF and roadmap-wave distribution
Source: created by Author.

Further methodological development is planned in three phases:

Phase 1. Construction of the model based on expert assessment and index-based approximation, which enables application of the framework to enterprises that do not have sufficient historical data on actual losses.

Phase 2. Calibration of the model based on accumulated empirical data, results of practical application of the framework and expert validation of the obtained estimates.

Phase 3. Construction of a statistically grounded model based on historical data on risk events and financial losses of enterprises. This stage is expected to become feasible after a sufficient volume of data has been accumulated, approximately within 18 months after the start of systematic data collection.

Conclusions. The article presented and substantiated the RR-framework 3.0 - an open, spreadsheet-based model that integrates the assessment of process maturity, digitalization and organizational resilience into one transparent computational chain and converts a structured self-assessment into crisis exposure, prioritized risks, strategy packages and an executable, economically sequenced roadmap. The study showed that the principal value of the model lies in closing the integration gap identified in the literature: it links staged maturity scoring with confidence adjustment, industry-specific gap analysis, a risk engine of score-specific treatments, crisis-scenario adjustment, a fuzzy resilience posture, WSJF-based initiative prioritization and analytic plus Monte Carlo-based tail-risk exposure approximation within a single, macro-free and reproducible artifact.

The demonstration case confirmed the operational coherence of the chain: from 424 questions the model produced an overall maturity of 2.25 of 5, identified Cyber Privacy, IT Cloud & DR and related domains as the dominant exposures under a severe ransomware scenario, quantified the corresponding tail risk, and translated the diagnosis into a prioritized 90-day-first roadmap led by compliance, dependency-mapping and data-protection initiatives. The practical value of these results is that organizations - especially small and medium-sized ones without access to bespoke consulting - obtain a free, transparent and methodologically grounded instrument that connects diagnostics directly to decisions, thereby strengthening the evidentiary basis of crisis management and digital transformation. Further research will focus on empirical calibration of industry templates and crisis multipliers, on benchmarking against panel data, and on extending the model toward continuous, data-fed assessment.

Declaration on the Use of Artificial Intelligence. During the preparation of this article, the author used AI-assisted tools in a supportive and non-substitutive manner: OpenAI ChatGPT, GPT-5.5 Thinking model, and Anthropic Claude Co-work Opus 4.8. These tools were used for auxiliary tasks, including language editing, translation support, improvement of clarity and structure, checking the consistency of formulations, assistance in verifying formulas and internal logic, preliminary search and organization of relevant materials, support in testing and documenting the RR-framework.

The AI-assisted tools were not used as autonomous au-

thors and did not replace the author's scientific contribution. All conceptual decisions, research design, methodological assumptions, development and testing of the RR-framework, selection and verification of sources, interpretation of results, and final conclusions were made, reviewed, and approved by the author, who bears full responsibility for the content of the article.

References:

1. World Economic Forum. (2024). The global risks report 2024 (19th ed.). https://www.weforum.org/publications/global-risks-report-2024
2. Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47–61. https://doi.org/10.1016/j.ress.2015.08.006
3. Sheffi, Y. (2005). The resilient enterprise: Overcoming vulnerability for competitive advantage. MIT Press.
4. Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Review Press.
5. Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2017). Achieving digital maturity. MIT Sloan Management Review and Deloitte. https://sloanreview.mit.edu/projects/achieving-digital-maturity
6. International Organization for Standardization. (2019). Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019).
7. International Organization for Standardization. (2018). Risk management - Guidelines (ISO 31000:2018).
8. Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. Omega, 62, 1–18. https://doi.org/10.1016/j.omega.2015.08.004
9. Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7
10. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kroeger, W., & Thiel-Clemen, T. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407–409. https://doi.org/10.1038/nclimate2227
11. Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. IEEE Software, 10(4), 18–27. https://doi.org/10.1109/52.219617
12. Becker, J., Knackstedt, R., & Poeppelbuss, J. (2009). Developing maturity models for IT management. Business & Information Systems Engineering, 1(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5
13. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z
14. Reznikov, R. (2023). The economic impact of cloud technologies on the Industry 4.0 development. Economic Herald of the Donbas, 4(74), 67–74. https://doi.org/10.12958/1817-3772-2023-4(74)-67-74
15. Reznikov, R. (2024a). Leveraging generative AI: Strategic adoption patterns for enterprises [Working paper]. SSRN. https://doi.org/10.2139/ssrn.4851632
16. Reznikov, R. (2024b). Crisis typology and taxonomy for IT service companies [Working paper]. SSRN. https://doi.org/10.2139/ssrn.4858983
17. Reznikov, R. (2024c). Navigating corporate turbulence: Strategies for managing companies during crisis. Investytsiyi: Praktyka ta Dosvid, (11), 95–100. https://doi.org/10.32702/2306-6814.2024.11.95
18. Reinertsen, D. G. (2009). The principles of product development flow: Second generation lean product development. Celeritas Publishing.
19. Zadeh, L. A. (1965). Fuzzy sets. Information and Control, 8(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X
20. Artzner, P., Delbaen, F., Eber, J.-M., & Heath, D. (1999). Coherent measures of risk. Mathematical Finance, 9(3), 203–228. https://doi.org/10.1111/1467-9965.00068
21. Rockafellar, R. T., & Uryasev, S. (2000). Optimization of conditional value-at-risk. Journal of Risk, 2(3), 21–41. https://doi.org/10.21314/JOR.2000.038
22. Reznikov, R. (2026). RR-framework v3.0: Business resilience and digital maturity assessment workbook [Computer software]. Zenodo. https://doi.org/10.5281/zenodo.20583866

Список використаних джерел:

1. The Global Risks Report 2024. 19th ed. Geneva : World Economic Forum, 2024. 124 p. URL: https://www.weforum.org/publications/global-risks-report-2024 (дата звернення: 24.05.2026).
2. Hosseini S., Barker K., Ramirez-Marquez J. E. A review of definitions and measures of system resilience. Reliability Engineering & System Safety. 2016. Vol. 145. Pp. 47–61. DOI: https://doi.org/10.1016/j.ress.2015.08.006
3. Sheffi Y. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. Cambridge, MA : MIT Press, 2005. 318 p.
4. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology into Business Transformation. Boston, MA : Harvard Business Review Press, 2014. 292 p.
5. Kane G. C., Palmer D., Phillips A. N., Kiron D., Buckley N. Achieving digital maturity. MIT Sloan Management Review and Deloitte. 2017. 31 p. URL: https://sloanreview.mit.edu/projects/achieving-digital-maturity (дата

звернення: 24.05.2026).

6. ISO 22301:2019. Security and resilience - Business continuity management systems - Requirements. Geneva : International Organization for Standardization, 2019. 28 p.

7. ISO 31000:2018. Risk management - Guidelines. Geneva : International Organization for Standardization, 2018. 16 p.

8. Annarelli A., Nonino F. Strategic and operational management of organizational resilience: current state of research and future directions. Omega. 2016. Vol. 62. Pp. 1–18. DOI: https://doi.org/10.1016/j.omega.2015.08.004

9. Duchek S. Organizational resilience: a capability-based conceptualization. Business Research. 2020. Vol. 13, No. 1. Pp. 215–246. DOI: https://doi.org/10.1007/s40685-019-0085-7

10. Linkov I., Bridges T., Creutzig F. et al. Changing the resilience paradigm. Nature Climate Change. 2014. Vol. 4, No. 6. Pp. 407–409. DOI: https://doi.org/10.1038/nclimate2227

11. Paulk M. C., Curtis B., Chrissis M. B., Weber C. V. Capability maturity model, version 1.1. IEEE Software. 1993. Vol. 10, No. 4. Pp. 18–27. DOI: https://doi.org/10.1109/52.219617

12. Becker J., Knackstedt R., Poeppelbuss J. Developing maturity models for IT management. Business & Information Systems Engineering. 2009. Vol. 1, No. 3. Pp. 213–222. DOI: https://doi.org/10.1007/s12599-009-0044-5

13. Teece D. J., Pisano G., Shuen A. Dynamic capabilities and strategic management. Strategic Management Journal. 1997. Vol. 18, No. 7. Pp. 509–533. DOI: https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

14. Reznikov R. The economic impact of cloud technologies on the Industry 4.0 development. Economic Herald of the Donbas. 2023. No. 4(74). Pp. 67–74. DOI: https://doi.org/10.12958/1817-3772-2023-4(74)-67-74

15. Reznikov R. Leveraging generative AI: strategic adoption patterns for enterprises. SSRN Working Paper. 2024. 7 p. DOI: https://doi.org/10.2139/ssrn.4851632

16. Reznikov R. Crisis typology and taxonomy for IT service companies. SSRN Working Paper. 2024. 5 p. DOI: https://doi.org/10.2139/ssrn.4858983

17. Reznikov R. Navigating corporate turbulence: strategies for managing companies during crisis. Інвестиції: практика та досвід. 2024. № 11. Pp. 95–100. DOI: https://doi.org/10.32702/2306-6814.2024.11.95

18. Reinertsen D. G. The Principles of Product Development Flow: Second Generation Lean Product Development. Redondo Beach, CA : Celeritas Publishing, 2009. 294 p.

19. Zadeh L. A. Fuzzy sets. Information and Control. 1965. Vol. 8, No. 3. Pp. 338–353. DOI: https://doi.org/10.1016/S0019-9958(65)90241-X

20. Artzner P., Delbaen F., Eber J.-M., Heath D. Coherent measures of risk. Mathematical Finance. 1999. Vol. 9, No. 3. Pp. 203–228. DOI: https://doi.org/10.1111/1467-9965.00068

21. Rockafellar R. T., Uryasev S. Optimization of conditional value-at-risk. Journal of Risk. 2000. Vol. 2, No. 3. Pp. 21–41. DOI: https://doi.org/10.21314/JOR.2000.038

22. Reznikov R. RR-framework v3.0: business resilience and digital maturity assessment workbook. Zenodo. 2026. DOI: https://doi.org/10.5281/zenodo.20583866

Дата надходження статті: 28.05.2026 р.
Дата прийняття статті до друку: 18.06.2026 р.
Дата публікації (оприлюднення) статті: 23.07.2026 р.