DOI: https://doi.org/10.32782/2524-0072/2026-88-44

UDC 005.334:005.21:004.9

DIGITAL MATURITY: EVIDENCE FROM A 24-COMPANY ASSESSMENT WITH THE RR-FRAMEWORK

МІЖГАЛУЗЕВА ДІАГНОСТИКА БІЗНЕС-СТІЙКОСТІ ТА ЦИФРОВОЇ ЗРІЛОСТІ: ЕМПІРИЧНІ РЕЗУЛЬТАТИ ОЦІНЮВАННЯ 24 КОМПАНІЙ ЗА ДОПОМОГОЮ RR-FRAMEWORK

Reznikov Roman
PhD in Economics,
Institute of Industrial Economics of the
National Academy of Sciences of Ukraine
ORCID: https://orcid.org/0000-0001-5581-5651

Резніков Роман Борисович
Інститут економіки промисловості
Національної академії наук України

The article presents a cross-industry empirical assessment of business resilience and digital maturity in twenty-four organizations using the RR-framework. The study addresses the need for reproducible diagnostics that connect maturity gaps with crisis exposure and prioritized action. The method combines a 424-item assessment across seventeen domains, confidence adjustment, crisis stress testing, fuzzy resilience posture, and analytic and Monte Carlo tail-risk estimation, followed by descriptive and correlation analysis. Results show mean maturity of 2.59 out of 5, an average of ten red-line breaches per organization, and a strong inverse relationship between maturity and modeled loss. Governance, cyber, IT continuity and workforce domains are identified as recurring weak spots. The study provides benchmarkable evidence for targeted resilience investment.

Keywords: business resilience, digital maturity, crisis management, risk assessment, cross-industry benchmarking, value-at-risk, maturity model, organizational diagnostics.

Статтю присвячено емпіричному міжгалузевому аналізу бізнес-стійкості та цифрової зрілості підприємств на основі структурованого оцінювання двадцяти чотирьох організацій, виконаного за допомогою інструменту RR-framework. Актуальність дослідження зумовлена потребою переходу від концептуальних моделей стійкості до відтворюваної, порівнянної та доказової діагностики, яка пов'язує розриви зрілості з кількісно вираженою кризовою експозицією та пріоритизованими діями. Метою роботи є перевірка практичної корисності та розрізнювальної здатності відкритого інструменту оцінювання і формування міжгалузевих орієнтирів стійкості на основі реальних результатів його застосування. Методику дослідження становлять уніфіковане оцінювання за 424 запитаннями у сімнадцяти бізнес-доменах, коригування на достовірність свідчень, стрес-тестування за кризовими сценаріями, нечіткий профіль стійкості, а також аналітичне й імітаційне (Монте-Карло) оцінювання хвостового ризику; одержані показники проаналізовано засобами описової статистики та кореляційного аналізу в межах усього портфеля. Результати засвідчують середній рівень загальної зрілості 2,59 з 5 за значного розкиду, у середньому десять порушень критичних контрольних меж на організацію та стійкі, послідовні зв'язки між зрілістю та ризиком: зрілість обернено пов'язана з кількістю порушень, цільовими розривами та модельованими хвостовими втратами, тоді як організації з найнижчою зрілістю несуть приблизно вшестеро більші модельовані втрати, ніж організації з найвищою зрілістю. Домени врядування й антикризового управління, кібербезпеки, безперервності інформаційних технологій і персоналу постають як системні слабкі місця незалежно від галузі. Практична цінність дослідження є подвійною: воно демонструє розрізнювальну здатність та придатність відкритого інструменту оцінювання для прийняття управлінських рішень, а також формує придатні до перенесення орієнтири, якими можуть скористатися підприємства, консультанти та органи влади для адресного спрямування інвестицій у стійкість і цифрову трансформацію.

Ключові слова: бізнес-стійкість, цифрова зрілість, антикризове управління, оцінювання ризиків, міжгалузевий бенчмаркінг, вартість під ризиком, модель зрілості, організаційна діагностика.

Statement of the problem. Business organizations increasingly operate in an environment of compound, fast-moving disruption – cyberattacks, supply-chain breakdowns, energy and liquidity shocks, regulatory change, pandemics and geopolitical escalation. Under such pressure, organizational resilience and digital maturity have become decisive determinants of survival and competitiveness [1, pp. 8–28; 2, pp. 47–61]. Yet most organizations still manage resilience qualitatively: they describe their capabilities in narrative terms, rarely measure them on a common scale, and almost never connect a maturity weakness to a quantified financial consequence. As a result, resilience investment is frequently misallocated – spread thinly, driven by the last incident, or concentrated where attention happens to fall rather than where exposure is greatest.

The practical task to which this study contributes is therefore the construction of reproducible, comparable and evidence-based diagnostics that turn a structured self-assessment into actionable, economically ranked priorities, and that allow results to be compared across organizations and industries. Comparability matters because isolated single-firm assessments cannot reveal which weaknesses are idiosyncratic and which are systemic; only a portfolio of consistently assessed organizations can establish benchmarks and expose patterns that individual reports conceal. This connects directly to important applied tasks of enterprise management, crisis preparedness and evidence-based economic policy, where decision-makers need defensible numbers rather than impressions. This need also complements international business-continuity and risk-management standards, which define systematic requirements and guidelines but do not provide a cross-industry benchmarking instrument [7, pp. 1–28; 8, pp. 1–16].

Analysis of recent research and publications. The study builds on four research streams. The measurement of organizational and system resilience has been systematized by Hosseini, Barker and Ramirez-Marquez, who showed that the field still lacks unified, operational metrics [2, pp. 47–61]; Annarelli and Nonino connected the strategic and operational dimensions of resilience management [3, pp. 1–18]; and Duchek framed resilience as a stage-wise capability of anticipation, coping and adaptation [4, pp. 215–246]. Linkov and co-authors argued for a shift from narrow risk analysis toward a resilience paradigm [5, pp. 407–409], and Sheffi demonstrated the competitive value of preparedness [6, pp. 1–318].

The maturity-model tradition provides the assessment paradigm. Since the Capability Maturity Model formalized staged improvement [9, pp. 18–27], maturity models have become a standard genre, and Becker, Knackstedt and Poeppelbuss codified the requirements for methodologically sound models [10, pp. 213–222]. The digital-transformation literature links maturity to performance: Westerman, Bonnet and McAfee established the empirical association between digital maturity and superior results [11, pp. 1–292], while Kane and colleagues identified strategy, culture and talent as the principal drivers of digital maturity [12, pp. 1–31]; Teece supplies the dynamic-capabilities foundation [13, pp. 509–533]. The author's prior work extends this stream to cloud technologies and Industry 4.0 [18, pp. 67–74], to generative artificial intelligence in enterprises [21, pp. 1–7], and to the typology and management of crises in technology firms [19, pp. 1–5; 20, pp. 95–100]. Finally, the quantitative apparatus comes from Reinertsen's WSJF prioritization [14, pp. 1–294], Zadeh's fuzzy sets [15, pp. 338–353] and the coherent-risk and conditional-value-at-risk theory of Artzner and co-authors and of Rockafellar and Uryasev [16, pp. 203–228; 17, pp. 21–41].

Highlighting previously unresolved parts of the overall problem. Two limitations of the existing literature define the unsolved part of the problem. First, these streams remain largely separate: maturity scores are rarely linked to quantified crisis exposure, and resilience assessments seldom terminate in an economically sequenced plan. Second, and more importantly for the present study, the empirical evidence is dominated by single-organization case studies and conceptual frameworks; there is a shortage of multi-organization, cross-industry evidence produced with one consistent, transparent instrument that would allow resilience and digital-maturity results to be compared and benchmarked. Without such evidence, claims about the usefulness of any assessment tool remain assertions. This article addresses that gap by applying a single open instrument – the RR-framework [22] – uniformly to twenty-four organizations and analysing the resulting portfolio.

Formation of the objectives of the article (task statement). The goal of the article is to obtain and analyse cross-industry empirical evidence on business resilience and digital

maturity produced with the RR-framework, and on that basis to assess the practical usefulness and discriminant validity of the instrument. The research tasks are: (1) to describe the assessment design and the portfolio of twenty-four organizations; (2) to present the portfolio-level distribution of maturity, gaps, control breaches and modeled tail risk; (3) to test the relationships among maturity, breaches, target gaps, crisis severity and modeled loss; (4) to identify systemic, cross-industry domain weaknesses and the recommended strategic responses; and (5) to draw conclusions on the analytical and managerial value of the instrument.

Summary of the main research material. Assessment design and data. The empirical base is a portfolio of twenty-four organizations assessed with a single, identical instrument – the RR-framework workbook [22] – under controlled conditions. Each organization answered the same 424 questions across seventeen business domains and seventy-six subdomains; every case is complete (424 answers, no blanks). The portfolio is deliberately heterogeneous, spanning SaaS and digital products, manufacturing, retail and e-commerce, financial services and fintech, healthcare and life sciences, energy and utilities, IT and connectivity services, logistics, the public sector, professional services, hospitality, media, mining and an NGO. Each organization was stress-tested against a relevant crisis scenario at a defined severity (from a calm baseline at severity 1 to extreme events at severity 5), so that the sample captures a wide range of both capability and threat. For every case the workbook produced an overall confidence-adjusted maturity, a benchmark percentile, an average gap to industry target, a count of red-line control breaches, a fuzzy resilience posture, a recommended primary strategy and analytic and Monte Carlo estimates of resilience loss (value-at-risk). The methodological components are grounded in WSJF prioritization, fuzzy-set theory, and coherent and conditional value-at-risk approaches [14, pp. 1–294; 15, pp. 338–353; 16, pp. 203–228; 17, pp. 21–41]. The overall maturity index of each organization is the confidence-weighted aggregate of its domain score:

$$M = \Sigma(\text{Domain Score}\_d \times \text{Weight}\_d) \,/\, \Sigma(\text{Weight}\_d) \quad (1)$$

Relationships across the portfolio are examined with the Pearson correlation coefficient as implemented in the RR-framework [22], which for two indicators X and Y over the n organizations is

$$r = \Sigma\left[(X\_i - \bar{X})(Y\_i - \bar{Y})\right] / \sqrt{\Sigma(X\_i - \bar{X})^2 \times \Sigma(Y\_i - \bar{Y})^2} \quad (2)$$

Portfolio-level results. Across the twenty-four organizations the mean overall maturity is 2.59 of 5 with a standard deviation of 0.75, ranging from 1.00 to 4.12 – a spread of more than three maturity levels that confirms the instrument discriminates sharply between weak and strong organizations. The average gap to industry target is 1.81 levels, and organizations accumulate, on average, ten red-line control breaches each, for a portfolio total of 240 breaches; the modeled 95% value-at-risk averages about 82.6 thousand index units. The descriptive statistics and the key correlations are summarized in Table 1.

The associations among the indicators are strong and internally consistent. Maturity is almost perfectly inversely related to the average target gap ($r = -0.99$), strongly inversely related to the number of red-line breaches ($r = -0.91$) and to modeled tail loss ($r = -0.93$), while modeled loss rises with both the number of breaches ($r = 0.93$) and crisis severity ($r = 0.67$). In other words, more mature organizations simultaneously show smaller gaps, fewer control breaches and lower modeled loss – exactly the coherence one would require of a valid diagnostic instrument. The distribution of overall maturity across the portfolio is shown in Figure 1, where organizations are coloured by maturity tier; the five lowest-scoring organizations fall below 2.0,

Table 1

Descriptive statistics of the 24-organization portfolio

Indicator	Mean	SD	Min	Max
Overall maturity (0–5)	2.59	0.75	1.00	4.12
Benchmark percentile	56	—	16	88
Average gap to target	1.81	—	0.04	3.65
Red-line breaches (count)	10.0	—	0	17
Modeled VaR 95% (index units)	82,565	—	15,508	136,959

Source: generated by the authors

sixteen occupy the 2.0–3.5 band, and only three exceed 3.5.

The maturity–risk relationship is displayed directly in Figure 2, which plots modeled value-at-risk against overall maturity, with bubble size and colour encoding crisis severity. The downward slope is unambiguous: as maturity rises, modeled tail loss falls steeply, and the residual scatter is explained largely by severity – for a given maturity, higher-severity scenarios sit higher on the loss axis. This is precisely the behaviour expected of a coherent instrument, in which both capability and threat move the risk estimate in the right direction.

Systemic, cross-industry weaknesses. Aggregating domain-level results across the portfolio exposes weaknesses that no single report could establish as systemic. Figure 3 ranks the business domains by how often they breach their red-line floor across the twenty-four organizations, overlaid with the average domain maturity. Governance & crisis management and cyber & privacy breach in twenty-one of twenty-four organizations, followed by IT cloud & disaster recovery and business systems (eighteen each) and the workforce domain (sixteen). The lowest average maturities are concentrated in physical safety, manufacturing execution, supply chain, workforce and governance. The convergence of these two views is the central diagnostic finding: governance, cyber, IT continuity and workforce are not company-specific blind spots but structural weaknesses that recur regardless of industry, and they are therefore strong candidates for sector-wide and policy-level attention. This interpretation is consistent with research emphasizing governance, preparedness, digital strategy, culture and talent as core dimensions of resilience and maturity [3, pp. 1–18; 4, pp. 215–246; 6, pp. 1–318; 12, pp. 1–31].

Resilience posture and strategic response. Translating maturity and exposure into a resilience posture, the instrument classifies thirteen of the twenty-four organizations as Exposed, seven as Adaptive, three as Resilient and one as Fragile (Figure 4, left). The dominance of the Exposed state is consistent with the portfolio-wide maturity deficit and the high breach

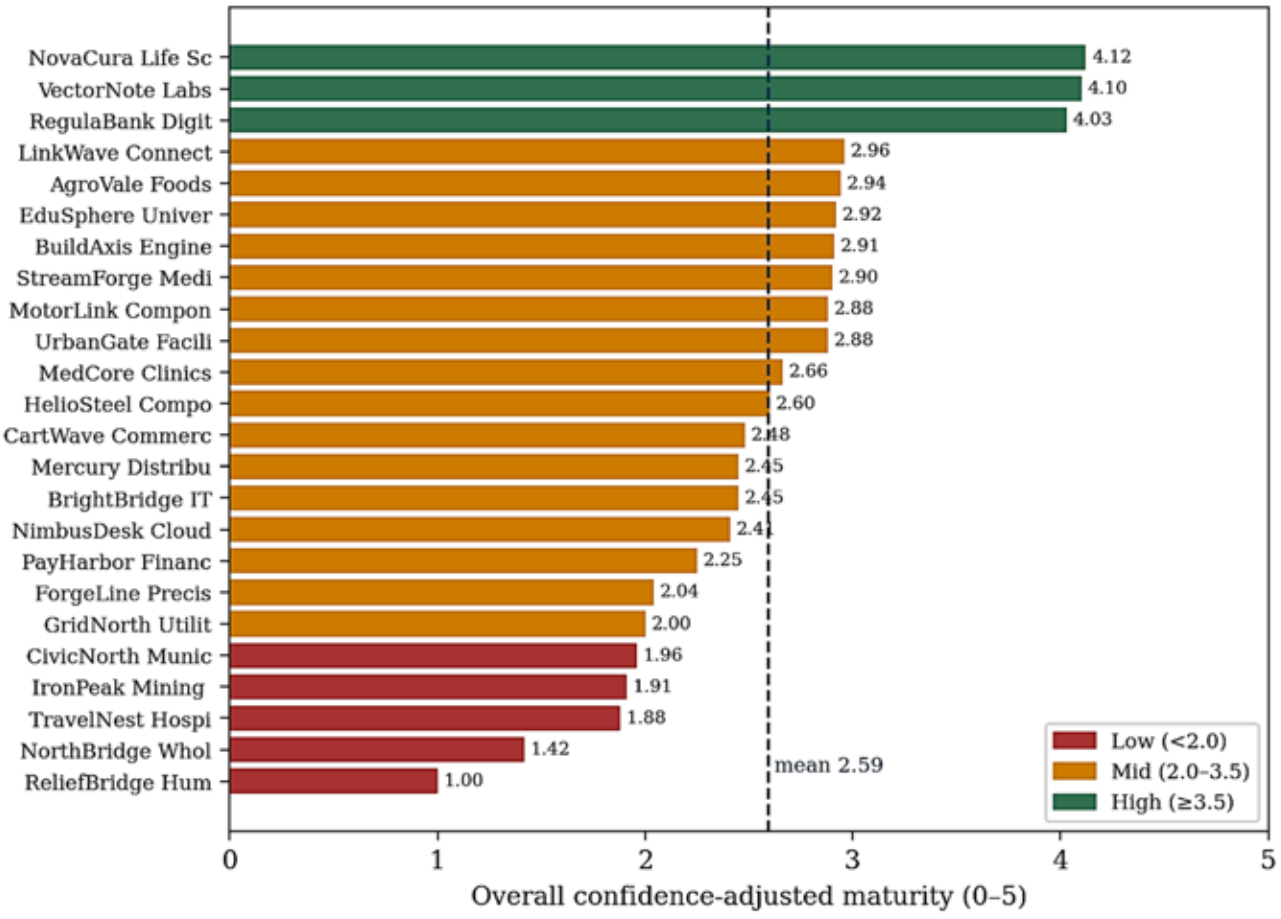

Figure 1. Overall maturity across the 24 assessed organizations

Source: generated by the author

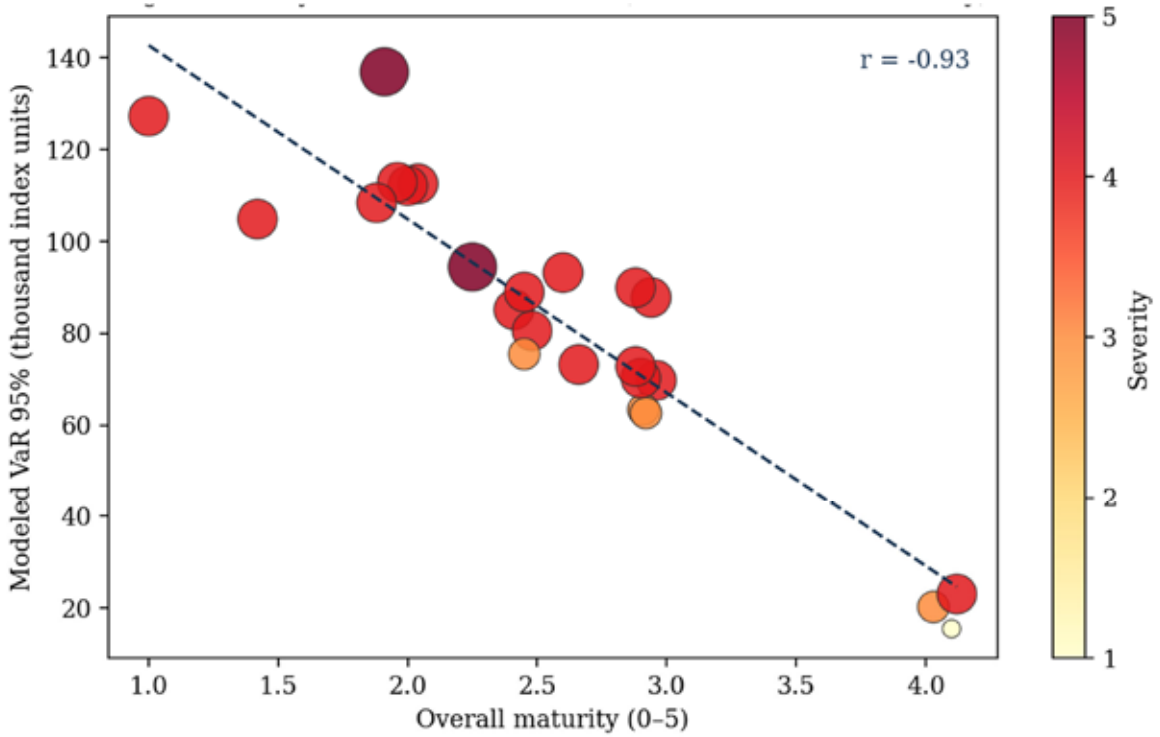

Figure 2. Maturity versus modeled tail risk across the portfolio (bubble size = crisis severity)

Source: generated by the author

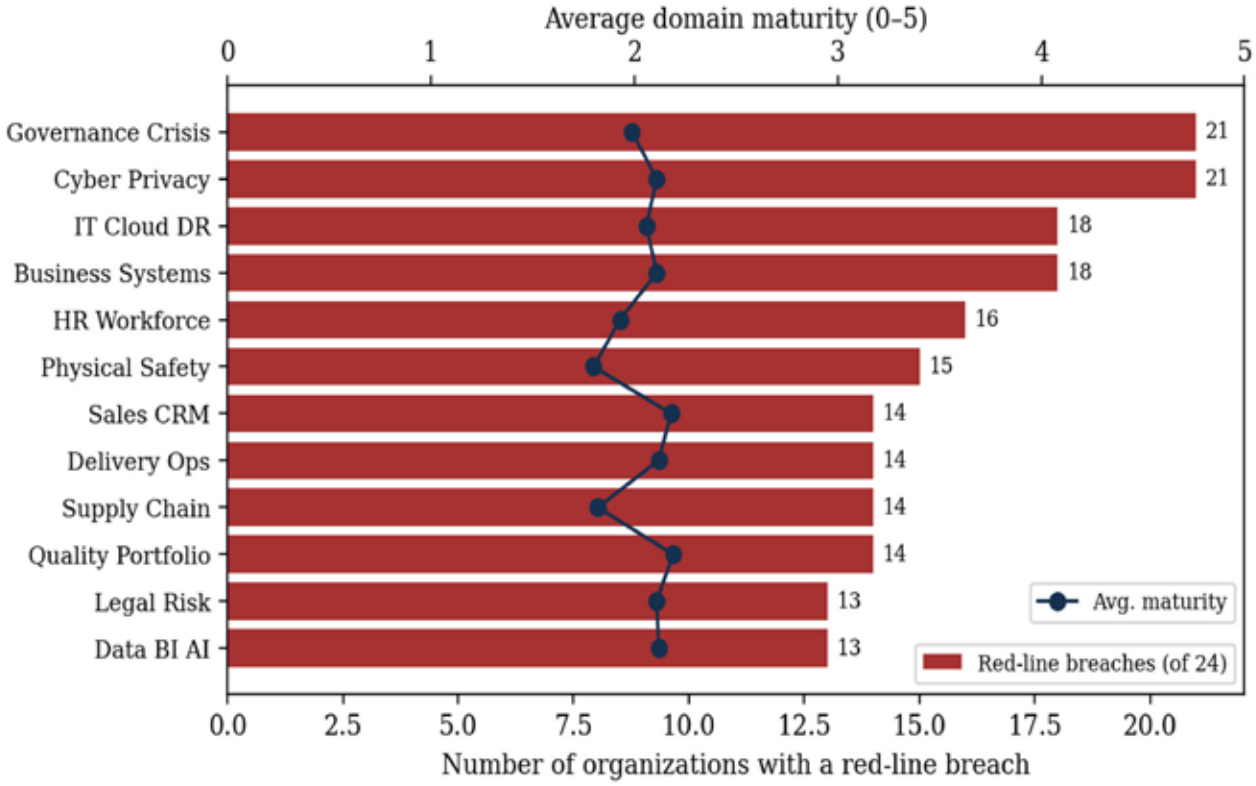

Figure 3. Systemic domain weaknesses across the portfolio (breach frequency and average maturity)

Source: generated by the author

Table 2

Per-organization assessment results (24 cases)

#	Company	Industry	Sev.	Mat.	Brch	VaR95	Posture
1	NimbusDesk	SaaS	4	2.41	9	85k	Exposed
2	VectorNote	SaaS	1	4.10	0	16k	Resilient
3	ForgeLine	Mfg.	4	2.04	17	113k	Exposed
4	HelioSteel	Mfg.	4	2.60	8	93k	Exposed
5	CartWave	Retail / E-comm.	4	2.48	12	81k	Exposed
6	NorthBridge	Retail / E-comm.	4	1.42	16	105k	Exposed
7	PayHarbor	Fintech	5	2.25	13	94k	Exposed
8	RegulaBank	Financial Serv	3	4.03	0	20k	Resilient
9	MedCore	Healthcare	4	2.66	11	73k	Exposed
10	GridNorth	Energy/Util.	4	2.00	17	112k	Exposed
11	BrightBridge	IT services	3	2.45	10	75k	Exposed
12	Mercury	Logistics	4	2.45	12	89k	Exposed
13	AgroVale	Mfg.	4	2.94	9	88k	Adaptive
14	LinkWave	IT services	4	2.96	8	70k	Adaptive
15	CivicNorth	Public sector	4	1.96	16	113k	Exposed
16	BuildAxis	Prof. serv.	3	2.91	4	63k	Adaptive
17	NovaCura	Life sci.	4	4.12	0	23k	Resilient
18	EduSphere	Public sector	3	2.92	8	63k	Adaptive
19	TravelNest	Prof. serv.	4	1.88	15	108k	Exposed
20	StreamForge	SaaS	4	2.90	9	70k	Adaptive
21	IronPeak	Mfg.	5	1.91	17	137k	Exposed
22	UrbanGate	Prof. serv.	4	2.88	3	73k	Adaptive
23	ReliefBridge	Public sector	4	1.00	16	127k	Fragile
24	MotorLink	Mfg.	4	2.88	10	90k	Adaptive

Source: generated by the author

counts. On the strategic side, the recommended primary strategy varies meaningfully with each organization's profile and crisis (Figure 4, right): a supply-chain and delivery resilience strategy is recommended most often (eight organizations), followed by cyber resilience, compliance and risk control, and workforce resilience strategies. The variation matters: it shows that the instrument does not issue a generic recommendation but tailors the response to the organization's specific weaknesses and threat, which is essential if the diagnosis is to drive differentiated action. The economic sequencing of responses follows WSJF prioritization logic [14, pp. 1–294] and the RR-framework methodology [22].

Discriminant validity and decision-usefulness. The clearest evidence of the instrument's value is the monotonic relationship between maturity tier and consequence. Grouping the organizations into low (overall maturity below 2.0; five organizations), mid (2.0–3.5; sixteen) and high (3.5 and above; three) tiers reveals a sharp gradient (Figure 5): average modeled value-at-risk falls from about 118 thousand index units in the low tier to about 83 thousand in the mid tier and to about 20 thousand in the high tier, while average red-line breaches fall from sixteen to ten to zero. The highest-maturity organizations thus carry roughly one-sixth of the modeled loss of the lowest-maturity ones and exhibit no red-line breaches at all. Two implications follow. First, the instrument has discriminant validity: organizations that differ in maturity differ predictably and substantially in modeled risk, so the score is informative rather than cosmetic. Second, the result quantifies the economic return to maturity, giving managers a concrete, defensible argument for resilience

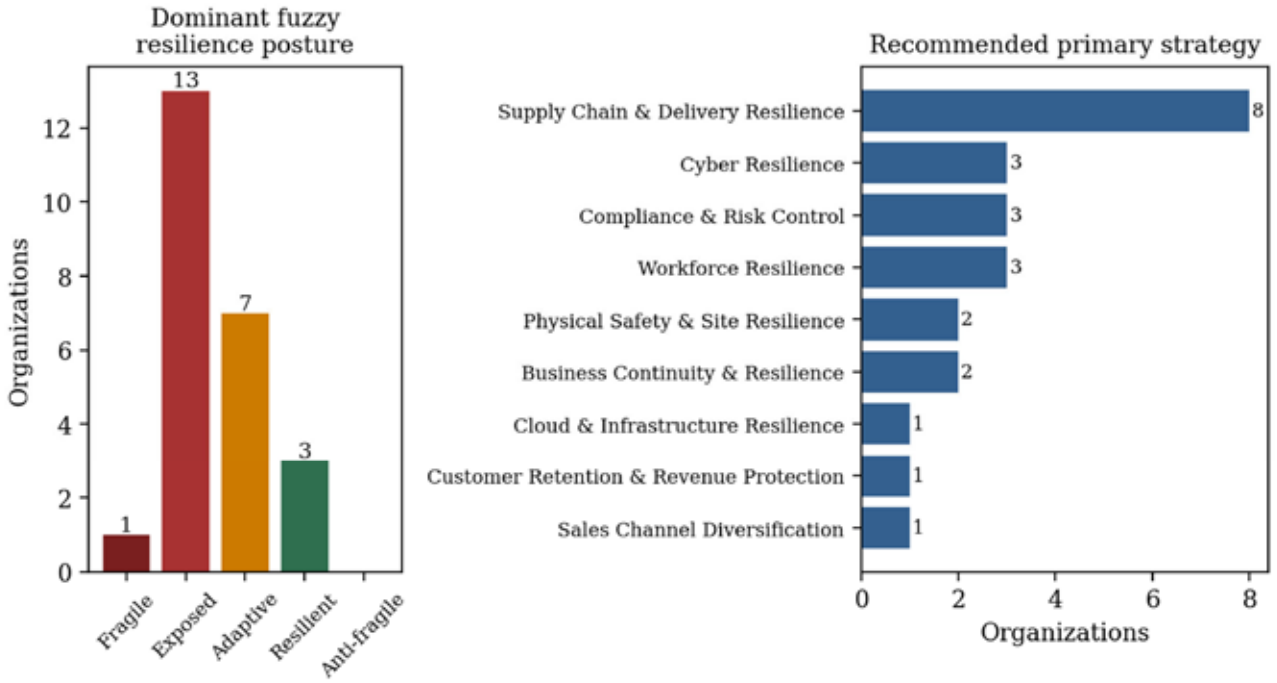

Figure 4. Dominant resilience posture and recommended primary strategy across the portfolio

Source: generated by the author

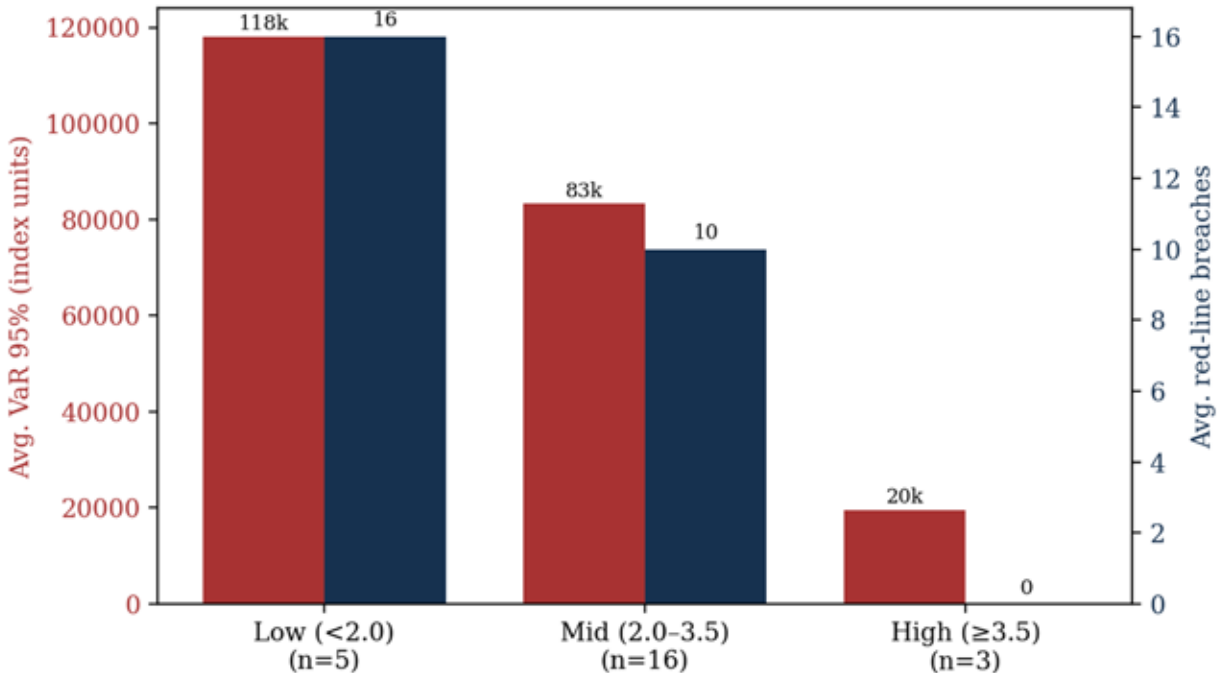

Figure 5. Maturity tier versus average modeled loss and control breaches

Source: generated by the author

investment and a way to target it where the modeled loss reduction is largest.

Taken together, the portfolio analysis substantiates four claims about the usefulness of the RR-framework as an analytical and managerial instrument. It is consistent – the strong, theory-conforming correlations among maturity, gaps, breaches and loss indicate that the model behaves coherently across very different organizations. It is discriminating – a three-

level spread in maturity and a sixfold spread in modeled loss show that it separates weak from strong organizations rather than compressing them toward a mean. It is comparable – because every organization is assessed with the same 424-item instrument, results can be benchmarked and aggregated, turning isolated diagnostics into portfolio intelligence and surfacing systemic weaknesses. And it is actionable – each assessment terminates in a fuzzy posture, a tailored strategy and an economically ranked roadmap, so the diagnosis converts directly into prioritized decisions. These properties are exactly those that an evidence-based resilience instrument must possess, and they are demonstrated here on real, reproducible output rather than asserted. These properties correspond to the methodological requirements for sound maturity models [9, pp. 18–27; 10, pp. 213–222].

The analysis also has limitations that delimit the conclusions. The portfolio, although deliberately heterogeneous, is a calibration sample of twenty-four synthetic but internally consistent organizations, so the correlations should be read as evidence of the instrument's internal coherence and discriminant behaviour rather than as population estimates for any real economy. The maturity inputs are self-assessed, and the loss figures are index-based approximations rather than firm-specific actuarial losses. These limitations do not weaken the central finding – that the instrument produces consistent, discriminating, comparable and actionable diagnostics – but they define the agenda for validation on larger, real-world samples.

Conclusions. The article reported a cross-industry empirical analysis of business resilience and digital maturity based on a uniform assessment of twenty-four organizations with the RR-framework. The portfolio shows a mean overall maturity of 2.59 of 5 with wide dispersion, an average of ten red-line control breaches per organization, and strong, internally consistent relationships in which maturity is inversely associated with target gaps ($r = -0.99$), control breaches ($r = -0.91$) and modeled tail loss ($r = -0.93$), while modeled loss rises with breaches ($r = 0.93$) and crisis severity ($r = 0.67$). Across industries, governance and crisis management, cyber and privacy, IT continuity and the workforce emerge as systemic weak spots, and the lowest-maturity organizations carry roughly six times the modeled loss of the highest-maturity ones.

The principal conclusion is that the instrument demonstrates discriminant validity and decision-usefulness: it produces consistent, discriminating, comparable and actionable diagnostics, and it quantifies the economic return to resilience maturity in a way that managers and policymakers can act on. The practical value is twofold – organizations obtain a transparent, free and benchmarkable instrument that connects diagnosis to prioritized investment, and the aggregated results yield transferable, cross-industry benchmarks for targeting resilience effort where modeled exposure is greatest. Prospects for further research include applying the instrument to larger samples of real organizations, validating the modeled loss estimates against observed incident data, extending the analysis to longitudinal re-assessment that tracks maturity improvement over time, and developing sector-specific benchmarks from the accumulated assessment base.

REFERENCES:

1. World Economic Forum. (2024). The global risks report 2024 (19th ed.). World Economic Forum. Retrieved June 25, 2026, from 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. Retrieved June 25, 2026, from https://doi.org/ 10.1016/j.ress.2015.08.006.

3. Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. *Omega*, 62, 1–18. Retrieved June 25, 2026, from https://doi.org/10.1016/j. omega.2015.08.004.

4. Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13(1), 215–246. Retrieved June 27, 2026, from https://doi.org/10.1007/s40685-019-0085-7.

5. 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. Retrieved June 25, 2026, from https://doi.org/ 10.1038/nclimate2227.

6. Sheffi, Y. (2005). The resilient enterprise: Overcoming vulnerability for competitive advantage. MIT Press.

7. International Organization for Standardization. (2019). Security and resilience — Business continuity management systems — Requirements (ISO 22301:2019).

8. International Organization for Standardization. (2018). Risk management — Guidelines (ISO 31000:2018).

9. Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE Software*, 10(4), 18–27. Retrieved June 25, 2026, from https://doi.org/10.1109/52.219617.

10. Becker, J., Knackstedt, R., & Poeppelbuss, J. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering*, 1(3), 213–222. Retrieved June 25, 2026, from https://doi.org/10.1007/s12599-009-0044-5.

11. Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Review Press.

12. Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2017). Achieving digital maturity. *MIT Sloan Management Review* and Deloitte. Retrieved June 25, 2026, from https://sloanreview.mit.edu/projects/achieving-digital-maturity.

13. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. Retrieved June 25, 2026, from https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

14. Reinertsen, D. G. (2009). The principles of product development flow: Second generation lean product development. Celeritas Publishing.

15. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338–353. Retrieved June 25, 2026, from https://doi.org/10.1016/S0019-9958(65)90241-X.

16. Artzner, P., Delbaen, F., Eber, J.-M., & Heath, D. (1999). Coherent measures of risk. *Mathematical Finance*, 9(3), 203–228. Retrieved June 25, 2026, from https://doi.org/10.1111/1467-9965.00068.

17. Rockafellar, R. T., & Uryasev, S. (2000). Optimization of conditional value-at-risk. *Journal of Risk*, 2(3), 21–41. Retrieved June 25, 2026, from https://doi.org/10.21314/JOR.2000.038.

18. Reznikov, R. (2023). The economic impact of cloud technologies on the Industry 4.0 development. *Economic Herald of the Donbas*, 4(74), 67–74. Retrieved June 25, 2026, from https://doi.org/10.12958/1817-3772-2023-4(74)-67-74.

19. Reznikov, R. (2024a). Crisis typology and taxonomy for IT service companies [Working paper]. SSRN. Retrieved June 25, 2026, from https://doi.org/10.2139/ssrn.4858983.

20. Reznikov, R. (2024b). Navigating corporate turbulence: Strategies for managing companies during crisis. *Investytsiyi: Praktyka ta Dosvid*, 11, 95–100. Retrieved June 25, 2026, from https://doi.org/10.32702/2306-6814.2024.11.95.

21. Reznikov, R. (2024c). Leveraging generative AI: Strategic adoption patterns for enterprises [Working paper]. SSRN. Retrieved June 25, 2026, from https://doi.org/10.2139/ssrn.4851632.

22. Reznikov, R. (2026). RR-framework v3.0: Business resilience and digital maturity assessment workbook [Computer software]. Zenodo. Retrieved June 25, 2026, from https://doi.org/10.5281/zenodo.20583866.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. World Economic Forum. 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: 25.06.2026).

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. P. 47–61. DOI: https://doi.org/10.1016/j.ress.2015.08.006 (дата звернення: 25.06.2026).

3. Annarelli A., Nonino F. Strategic and operational management of organizational resilience: current state of research and future directions. *Omega*. 2016. Vol. 62. P. 1–18. DOI: https://doi.org/10.1016/j.omega.2015.08.004 (дата звернення: 25.06.2026).

4. Duchek S. Organizational resilience: a capability-based conceptualization. *Business Research*. 2020. Vol. 13, No. 1. P. 215–246. DOI: https://doi.org/10.1007/s40685-019-0085-7 (дата звернення: 25.06.2026).

5. Linkov I., Bridges T., Creutzig F. et al. Changing the resilience paradigm. *Nature Climate Change*. 2014. Vol. 4, No. 6. P. 407–409. DOI: https://doi.org/10.1038/nclimate2227 (дата звернення: 25.06.2026).

6. Sheffi Y. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. Cambridge, MA : MIT Press, 2005. 318 p.

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

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

9. Paulk M. C., Curtis B., Chrissis M. B., Weber C. V. Capability maturity model, version 1.1. *IEEE Software*. 1993. Vol. 10, No. 4. P. 18–27. DOI: https://doi.org/10.1109/52.219617 (дата звернення: 25.06.2026).

10. Becker J., Knackstedt R., Poeppelbuss J. Developing maturity models for IT management. *Business & Information Systems Engineering*. 2009. Vol. 1, No. 3. P. 213–222. DOI: https://doi.org/10.1007/s12599-009-0044-5 (дата звернення: 25.06.2026).

11. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology into Business Transformation. Boston, MA : Harvard Business Review Press, 2014. 292 p.

12. 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: 25.06.2026).

13. Teece D. J., Pisano G., Shuen A. Dynamic capabilities and strategic management. *Strategic Management Journal*. 1997. Vol. 18, No. 7. P. 509–533. DOI: https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z (дата звернення: 25.06.2026).

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

15. Zadeh L. A. Fuzzy sets. *Information and Control*. 1965. Vol. 8, No. 3. P. 338–353. DOI: https://doi.org/10.1016/S0019-9958(65)90241-X (дата звернення: 25.06.2026).

16. Artzner P., Delbaen F., Eber J.-M., Heath D. Coherent measures of risk. *Mathematical Finance*. 1999. Vol. 9, No. 3. P. 203–228. DOI: https://doi.org/10.1111/1467-9965.00068 (дата звернення: 25.06.2026).

17. Rockafellar R. T., Uryasev S. Optimization of conditional value-at-risk. *Journal of Risk*. 2000. Vol. 2, No. 3. P. 21–41. DOI: https://doi.org/10.21314/JOR.2000.038 (дата звернення: 25.06.2026).

18. Reznikov R. The economic impact of cloud technologies on the Industry 4.0 development. *Economic Herald of the Donbas*. 2023. No. 4(74). P. 67–74. DOI: https://doi.org/10.12958/1817-3772-2023-4(74)-67-74 (дата звернення: 27.06.2026).

19. Reznikov R. Crisis typology and taxonomy for IT service companies. SSRN Working Paper. 2024. 5 p. DOI: https://doi.org/10.2139/ssrn.4858983 (дата звернення: 25.06.2026).

20. Reznikov R. Navigating corporate turbulence: strategies for managing companies during crisis. *Інвестиції: практика та досвід*. 2024. № 11. P. 95–100. DOI: https://doi.org/10.32702/2306-6814.2024.11.95 (дата звернення: 27.06.2026).

21. Reznikov R. Leveraging generative AI: strategic adoption patterns for enterprises. SSRN Working Paper. 2024. 7 p. DOI: https://doi.org/10.2139/ssrn.4851632 (дата звернення: 25.06.2026).

22. Reznikov R. RR-framework v3.0: business resilience and digital maturity assessment workbook. Zenodo. 2026. DOI: https://doi.org/10.5281/zenodo.20583866. URL: https://github.com/RR009N/RR-framework (дата звернення: 25.06.2026).

Дата надходження статті: 27.06.2026
Дата прийняття статті до публікації: 17.08.2026
Дата публікації статті: 28.08.2026