Journal of Process Management and New Technologies
Vol. 14, Issue 3-4, 2026, pp. 15-28

A MATURITY-BASED READINESS MODEL FOR IMPLEMENTING DIGITAL FINANCIAL TECHNOLOGIES

Dragiša D. ŽUNIĆ[1,2*], Jasmina ĐURAŠKOVIĆ[3], Bojan STOILJKOVIĆ[4]

[1]*Institute for Artificial Intelligence R&D of Serbia, Novi Sad, Serbia, dragisa.zunic@ivi.ac.rs*
https://orcid.org/0000-0002-0345-6797

[2]*Gran Sasso Science Institute (GSSI), L'Aquila, Italy*

[3]*Academy of Applied Studies Polytechnic, Belgrade, Serbia, jdjuraskovic@politehnika.edu.rs*
https://orcid.org/0000-0001-6020-6025

[4]*Alfa BK University, Belgrade, Serbia, bojan.stoiljkovic@alfa.edu.rs*
https://orcid.org/0000-0003-2796-8663

Abstract: *Digital financial technologies are often discussed as technical innovations, although successful implementation depends on broader organizational readiness. The goal of this paper is to develop a compact model for assessing whether financial organizations are prepared to implement and operate such technologies responsibly. Using a conceptual model-building approach, the study synthesizes maturity-model design principles, digital-transformation research, operational-resilience guidance, and financial-technology risk literature. The resulting Digital Financial Technology Implementation Readiness Model (DFT-IRM) organizes readiness into five domains: technology and data, operational resilience, governance and strategy, risk and compliance, and people and adoption. It applies five cumulative maturity levels and combines a domain profile with a bottleneck readiness level and a secondary progress index; an optional target-based gap indicator supports more detailed prioritization. The analysis shows that technical progress alone cannot establish deployment readiness when critical organizational capabilities remain weak. DFT-IRM therefore offers a lightweight, evidence-oriented diagnostic framework for identifying implementation bottlenecks and guiding process improvement before weaknesses become operational, regulatory, or reputational failures.*

Keywords: *digital financial technology, implementation readiness, maturity model, operational resilience, governance, compliance*

Original scientific paper
Received: 20.07.2026
Accepted: 26.08.2026
Available online: 20.09.2026
DOI: 10.5937/jpmnt14-69402

1. Introduction

Financial organizations are under pressure to modernize faster than their internal capabilities can often support. Banks connect ageing core systems to new digital channels. Payment providers run increasingly data-intensive services. Investment firms rely on

* Corresponding author

automated platforms, cloud infrastructure, outsourced technology, and real-time reporting. Financial-market infrastructures must remain resilient under demanding operational and regulatory conditions. At the same time, blockchain-based finance introduces smart contracts, tokenized assets, decentralized applications, protocol governance, and new forms of automated financial service provision (Financial Stability Board, 2023; Schär, 2021; Werner et al., 2022).

Digital financial technologies do not form a single class of systems. Some are visible to the customer: a payment application, a mobile banking platform, or a service for trading tokenized assets. Others work behind the screen. They monitor transactions, calculate risk, support compliance, automate reporting, or help institutions make decisions. Still others are built around programmable infrastructures, including smart contracts, decentralized applications, automated market makers, and blockchain-based settlement or lending systems.

These systems differ in purpose, scale, and architecture. Yet the practical question is often the same. Can the organization operate the technology reliably, understand the data on which it depends, control the risks it creates, assign responsibility when something goes wrong, and support the people who must use it? DFT-IRM is intended to examine this wider condition of readiness. It therefore treats technical capability as necessary, but not sufficient.

These developments are usually described as digital transformation. In finance, however, implementation is not simply a matter of acquiring or deploying better technology. A new system may work correctly in a technical demonstration and still fail in practice because data are unreliable, responsibilities are unclear, operational teams are unprepared, compliance requirements have not been translated into controls, or users do not understand how the new service changes their work. Such weaknesses can quickly lead to operational losses, regulatory breaches, service interruptions, reputational damage, or wider disruption (Basel Committee on Banking Supervision, 2021; Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, 2012).

Existing digital-maturity models provide a useful starting point because they treat transformation as gradual, multidimensional, and organizational rather than merely technological (Becker et al., 2009; Pöppelbuß & Röglinger, 2011; Teichert, 2019). However, many remain too general for financial technologies implementation, and some imply more numerical precision than their supporting evidence gives (Thordsen & Bick, 2023; Thordsen et al., 2020).

Financial organizations face specific constraints: sensitive data, critical services, regulatory reporting, cyber risk, outsourcing, business-continuity obligations, operational resilience, and potentially rapid transmission of failures (Basel Committee on Banking Supervision, 2021; Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, 2012; Papathomas & Konteos, 2024). Decentralised finance adds a further complication because relevant responsibilities may be distributed across protocols, developers, validators, oracles, governance communities, interface providers, and users (Aramonte et al., 2021; Financial Stability Board, 2023; Schär, 2021; Werner et al., 2022).

Accordingly, this paper asks when a financial organization is genuinely ready to implement and operate digital financial technology. To address this question, the paper proposes the Digital Financial Technology Implementation Readiness Model (DFT-IRM). It is a lightweight, maturity-based model for assessing whether a financial organization is ready to implement and operate digital financial technology. Readiness is examined across five organizational domains: technology and data, operational resilience, governance and strategy, risk and compliance, and people and adoption.

The model rests on the proposition that financial organizations are not ready to implement digital financial technologies merely because the technology works. They are ready when the surrounding organization can operate, govern, monitor, recover, and adapt that technology responsibly.

The scope is intentionally modest. DFT-IRM is not presented as a statistically validated universal scale, and it does not certify products, rank firms, predict commercial success, or evaluate the economic quality of a financial service. Nor does it analyze market mechanisms, trading rules, exchange-core computation, matching logic, Reaction Systems, concurrent exchange models, or the economic design of financial protocols. Its contribution is organizational and process-oriented: a compact diagnostic framework for implementation readiness. This focus complements earlier work on formal models of market operation, which examines mechanism-level properties rather than organizational readiness (Cervesato et al., 2019; Žunić, 2023).

The distinctive feature of DFT-IRM is therefore not the use of maturity levels alone, but their combination with evidence-based assessment and a bottleneck-sensitive interpretation of implementation readiness. Therefore, the rest of the paper is organized as follows. Section 2 discusses related work. Section 3 describes the conceptual method. Section 4 presents the DFT-IRM domains, maturity levels, assessment method, and illustrative applications. Section 5 discusses the model in relation to conventional finance and decentralized finance and states its limitations, whereas in Section 6 conclusions are given.

2. Related work

The discussion draws on three bodies of literature: maturity-model research, financial-sector digital transformation and resilience, and decentralized-finance risk. Maturity models are widely used to describe staged development of organizational capabilities. Rather than treating transformation as a single decision or investment, they represent progress as movement through levels of increasing structure, control, and adaptation. Becker et al. (2009) emphasize that maturity-model development should follow a clear procedure and be oriented towards a defined application area. Pöppelbuß and Röglinger (2011) similarly stress that useful maturity models should have a clear purpose, transparent design principles, and practical value for improvement.

Digital-maturity literature extends this logic to organizational digital transformation. Teichert (2019) reviews digital transformation maturity and shows that the field is multidimensional, covering technology, strategy, organization, culture, and capabilities. However, critical evaluations also warn that maturity models can become too generic, weakly grounded, or presented with more precision than their evidence justifies (Thordsen & Bick, 2023; Thordsen et al., 2020). This caution is important for the present paper. DFT-IRM uses levels and scores, but it treats them as structured judgments supported by evidence, not as exact measurements. Recent work similarly treats digital readiness as a multidimensional organizational capability rather than a purely technological condition (Al-Omoush & Alsmadi, 2026; Silva et al., 2025).

Financial-sector literature shows why a domain-specific readiness model is useful. Digital transformation in financial institutions is not merely a technical upgrade. It involves business processes, regulatory obligations, operational capabilities, customer-facing services, cybersecurity, third-party dependencies, and strategic change (Papathomas & Konteos, 2024). International guidance on operational resilience, such as the Basel Committee's principles, also emphasizes governance, ICT risk, continuity, testing, response, recovery, and third-party dependency (Basel Committee on Banking Supervision, 2021). The CPSS-IOSCO principles for financial-market infrastructures similarly highlight governance, comprehensive risk management, operational reliability, and transparency (Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, 2012). Recent banking evidence further shows that digital transformation interacts with

uncertainty, operational efficiency, governance, and risk-taking rather than producing uniform outcomes (Dai & Song, 2026; Huynh, 2025; Wang et al., 2025; Yu & Liu, 2025).

A concrete case illustrates this point. The UBS ATS case was not only a matter of software functionality; it involved the relationship between design, implementation, documentation, disclosure, testing, and regulatory oversight (Ignatovich & Passmore, 2015). The broader lesson extends beyond exchanges: sophisticated financial technologies require coordinated capability across business, technology, quality assurance, compliance, risk management, and operations.

Decentralized finance adds another layer to the problem. Schär (2021) describes DeFi as a layered system of blockchain-based financial applications, while Werner et al. (2022) systematizes its technical and economic risks. The Financial Stability Board (2023) argues that DeFi retains many familiar vulnerabilities, and BIS research warns that decentralization may coexist with concentrations of influence and governance dependency (Aramonte et al., 2021). DeFi therefore does not remove readiness questions; it redistributes them.

DFT-IRM differs from broader maturity-model approaches by focusing on implementation readiness rather than organization-wide transformation or commercial benchmarking. General digital-maturity models usually span sectors and whole organizations. Banking-oriented models are closer to the present setting, but often emphasize digital channels, customer experience, business performance, or institutional comparison. DFT-IRM instead asks whether a financial organization is practically prepared to implement and operate a particular digital financial technology across the five defined domains. The resulting gap is narrow but important: existing digital-maturity models are useful but often too broad, while financial-technology literature rarely provides a compact diagnostic model for determining whether an organization is ready to implement and operate digital financial technology responsibly.

3. Methods

The study follows a conceptual model-building approach. It draws on maturity-model design principles, digital-transformation literature, operational-resilience guidance, and selected financial-technology risk literature (Becker et al., 2009; Pöppelbuß & Röglinger, 2011; Teichert, 2019). The purpose is not to create a statistically validated measurement instrument, but to develop a transparent diagnostic framework for implementation planning and organizational improvement.

Four design choices guide the construction of DFT-IRM:

First, the model is domain specific. It focuses on digital financial technology rather than digital transformation in general. This is necessary because financial organizations operate under stricter requirements for resilience, compliance, data protection, accountability, and continuity of critical services (Basel Committee on Banking Supervision, 2021; Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, 2012).

Second, the model is multidimensional. It does not reduce readiness to technical capability. It treats implementation as a combination of technology, operations, governance, risk, compliance, and adoption. This is consistent with the broader digital-maturity literature, which treats digital transformation as a multidimensional organizational process (Teichert, 2019; Thordsen & Bick, 2023).

Third, the model is evidence oriented. Maturity levels should be supported by observable evidence, such as procedures, test results, audit trails, training records, governance decisions, incident reports, recovery exercises, or control documentation. This design choice responds to the general maturity-model requirement that assessment criteria should be transparent and practically useful (Pöppelbuß & Röglinger, 2011).

The strength of that evidence should reflect both the criticality of the technology and the property being assessed. Testing can reveal defects in the executions examined, but cannot in general establish their absence (Dijkstra, 1972). Formal methods can provide stronger assurance for precisely specified properties by reasoning over all behaviors represented by a formal model (Wing, 1990). Their conclusions nevertheless remain bound by the specification and assumptions used.

Fourth, the model is bottleneck sensitive. It does not allow strong performance in one domain to fully compensate for critical weakness in another. This is especially important in finance, where weak compliance, weak resilience, or weak governance may block responsible deployment even when the technology itself appears advanced (Basel Committee on Banking Supervision, 2021).

In practice, an assessment begins by defining the technology or service under consideration, identifying the evidence available in each domain, assigning the highest maturity level consistently supported by that evidence, and examining both the full profile and the weakest critical domain. The resulting profile is intended to guide discussion and prioritization rather than to produce a certification decision.

4. Results

4.1. DFT-IRM domains

DFT-IRM assesses implementation readiness across five connected domains. Together, they reflect the fact that digital financial technologies depend not only on software, but also on reliable data, resilient operation, accountable governance, embedded risk and compliance controls, and informed adoption by people. The five domains, their guiding questions, and examples of supporting evidence are summarized in Table 1.

Table 1. DFT-IRM domains, guiding questions, and typical evidence

Domain	Main question	Typical evidence
Technology and data readiness	Can the technical and data foundation support the service?	Architecture documents, integration tests, data-quality controls, cybersecurity tests, access-control design, capacity tests, dependency maps
Operational resilience	Can critical services continue or recover under disruption?	Monitoring procedures, incident-response plans, continuity tests, recovery exercises, escalation procedures, post-incident reviews
Governance and strategy	Are ownership, decision rights, and strategic objectives clear?	Role assignments, approval procedures, change-management records, budget decisions, risk-acceptance records
Risk and compliance	Are legal, regulatory, security, outsourcing, and conduct risks translated into controls?	Compliance mapping, audit trails, reporting procedures, outsourcing assessments, control documentation, regulatory evidence
People and adoption	Can staff and users operate the system responsibly?	Training records, user-support procedures, stakeholder communication, knowledge-transfer plans, adoption feedback

Source: Authors' elaboration

4.1.1. Technology and data readiness

This domain asks whether the technical and data foundation can support the proposed service. It includes architecture, interoperability, system capacity, cybersecurity, data quality, access controls, testing environments, documentation, and third-party technology dependencies.

Working software alone does not demonstrate readiness. The organization should understand where critical data originates, how they are validated, how systems exchange information, and what happens when an external provider or infrastructure component fails. In financial settings, this concern is reinforced by operational-resilience guidance and by the importance of reliable, secure, and sufficiently capacitated systems in financial-market infrastructures (Basel Committee on Banking Supervision, 2021; Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, 2012).

For critical components, relevant evidence may range from conventional testing and simulation to static analysis, model checking, or theorem-based verification, depending on the property and the required level of assurance. A recent payment-system study illustrates this use of model checking for formally specified process-flow properties (Janulevičius, 2026).

4.1.2. Operational resilience

This domain asks whether the organization can maintain or restore critical services under disruption. It includes monitoring, incident response, business continuity, backup arrangements, recovery objectives, escalation procedures, stress testing, and post-incident learning.

In finance, operational failure can affect customers, counterparties, supervisors, and connected institutions. Preparation for disruption therefore matters as much as evidence of normal operation. This view is consistent with the operational-resilience perspective, which treats response and recovery as core organizational capabilities rather than peripheral technical concerns (Basel Committee on Banking Supervision, 2021).

4.1.3. Governance and strategy

This domain asks whether ownership and decision rights are clear. A financial-technology project may have capable developers and still be immature if no one has authority to approve changes, stop deployment, resolve conflicting requirements, or accept residual risk.Governance readiness connects technical work with organizational accountability. It ensures that implementation is not only technically possible but also institutionally owned. In this way, the domain reflects the broader maturity-model principle that organizational improvement requires a clear target area, accountable users, and transparent criteria for action (Becker et al., 2009; Pöppelbuß & Röglinger, 2011). Recent evidence also links bank digital transformation with improved transparency through stronger internal governance and information quality (Zhang et al., 2025).

4.1.4. Risk and compliance

This domain asks whether legal, regulatory, security, outsourcing, model, and conduct risks are identified early and translated into operational controls. Compliance cannot be left to a final-stage approval exercise. It should shape data architecture, logging, reporting, access management, monitoring, documentation, vendor selection, and incident procedures throughout implementation. This domain also concerns the organization's ability to explain why a system was considered ready and what evidence supported that decision. The UBS ATS case illustrates why design, implementation, documentation, testing, and regulatory oversight

cannot be cleanly separated in sophisticated financial technologies (Ignatovich & Passmore, 2015). These concerns are particularly visible in algorithmic banking, where governance responsibilities, documentation standards, model risk, and accountability are central supervisory issues (García-Llorente & Olmeda, 2026).

4.1.5. People and adoption

This domain asks whether staff and users can operate the system responsibly. Digital transformation changes tasks, responsibilities, routines, and sometimes authority. A system can be technically sound and still fail because employees do not trust it, misunderstand its outputs, bypass controls, or lack the expertise to handle exceptional situations. Adoption readiness therefore concerns both competence and organizational acceptance. This is consistent with the broader view of digital transformation as an organizational journey rather than a purely technical upgrade (Papathomas & Konteos, 2024; Teichert, 2019).

4.2. Maturity levels and readiness assessment

DFT-IRM is maturity-based: it uses five cumulative maturity levels to assess implementation readiness. The five cumulative levels are summarized in Table 2.

Table 2. Cumulative maturity levels used in DFT-IRM

Level	Description
0 — Unprepared	Relevant capabilities are absent or largely unrecognised.
1 — Initiated	Some activities exist, but they are informal, fragmented, or reactive.
2 — Defined	Responsibilities, procedures, and minimum controls are documented.
3 — Managed	Capabilities are monitored, tested, measured, and systematically controlled.
4 — Adaptive	Evidence from operation, incidents, and environmental change is used for continual improvement.

Source: Authors' elaboration

The levels are cumulative. An organization should not be assessed at Level 3 in a domain when the basic Level 2 procedures are missing. For example, dashboards alone do not make operational capability managed if incident-response responsibilities are undocumented and recovery procedures remain untested.

Every score should be supported by observable evidence, such as approved procedures, completed tests, incident records, audit findings, training outcomes, recovery exercises, governance decisions, or documented control reviews. This matters because maturity levels are ordinal judgments rather than physical measurements. Critical evaluations of digital-maturity models caution against assigning more precision to maturity scores than the evidence can support (Thordsen & Bick, 2023; Thordsen et al., 2020).

An organization receives the maturity profile defined in Equation (1):

$$\mathrm{m}=(m_T,\mathrm{m}_O,\mathrm{m}_G,\mathrm{m}_R,\mathrm{m}_P) \tag{1}$$

where:

m_T is the readiness level for technology and data;
m_O is the readiness level for operational resilience;
m_G is the readiness level for governance and strategy;
m_R is the readiness level for risk and compliance;
m_P is the readiness level for people and adoption.

The profile is the main diagnostic result because it reveals uneven capability. A single average can conceal a serious weakness. For example:

$$\mathrm{m}=(4,4,4,1,4) \tag{2}$$

describes an organization with strong maturity in most domains but serious weakness in risk and compliance. It should not be treated as generally highly ready simply because its average score is high.

For this reason, Equation (3) summarizes readiness through three connected outputs:

$$\mathrm{Readiness}=(\mathrm{M},\mathrm{I},\mathrm{m}) \tag{3}$$

where:

M is the bottleneck readiness level;

I is the weighted progress index;

m is the full maturity profile.

Let C denote the set of domains identified as critical for the intended implementation. The bottleneck readiness level M is defined in Equation (4):

$$m_d \tag{4}$$

The weighted progress index I is defined in Equation (5):

$$\mathrm{I}=\sum_d w_d\, m_d, \sum_d w_d = 1 \tag{5}$$

The logic is simple. The profile m shows the full readiness picture. Bottleneck level M identifies the weakest critical domain. The progress index I show overall progress without replacing the bottleneck view. The bottleneck level prevents strong domains from fully compensating for critical weakness. This is especially important in finance, where one weak critical domain can block responsible deployment. Strong technology cannot fully compensate for absent compliance controls. Good governance cannot fully compensate for untested recovery procedures. Staff enthusiasm cannot compensate for unreliable data.

The progress index remains useful, but only as a secondary indicator. It can show whether an organization is generally improving, or whether two organizations with the same bottleneck level differ in overall preparation. However, it should not override the profile or the bottleneck assessment.

For applications requiring more detailed prioritization, Equations (6)–(8) introduce an optional target-based gap assessment. The target profile is:

$$\tau=(\tau_T,\tau_O,\tau_G,\tau_R,\tau_P) \tag{6}$$

where τ_d denotes the required maturity level for domain d. For example, an organization may decide that full production deployment requires at least Level 3 in all critical domains:

$$\tau = (3, 3, 3, 3, 3)$$

The positive gap in each domain is:

$$\mathrm{gap}_d=\max(0,\tau_d - m_d) \tag{7}$$

Thus, a domain above the target is not penalized, while a domain below the target contributes to the remaining implementation gap. A compact severity-adjusted gap indicator can then be defined as:

$$\mathrm{G}=\sum_d w_d\,[\max(0,\tau_d - m_d)]^2 \tag{8}$$

where w_d is the weight assigned to domain d and the domain weights sum to 1.

The squared term gives greater weight to serious weaknesses. A domain that is two levels below target is therefore treated as a more severe implementation deficiency than a domain that is only one level below target. This can help distinguish a project blocked by one serious weakness from a project affected by several moderate weaknesses.

This optional indicator should be used cautiously. Maturity levels are ordinal judgments supported by evidence, not exact physical measurements. Therefore, G should not be

interpreted as a precise quantitative risk score. It is better understood as a structured aid for prioritizing implementation improvements.

4.3. Illustrative applications

This section illustrates how DFT-IRM can be used to identify implementation bottlenecks. The examples are not empirical case studies. They are structured applications of the model to realistic financial-technology implementation scenarios.

4.3.1. Digital payments Pplatform with tokenized-asset functionality

Consider a mid-sized financial institution preparing to introduce a new digital payments platform. The platform connects to external service providers, supports automated reporting, and includes limited tokenized-asset functionality. Technically, the system has passed initial integration tests and the architecture is documented. However, the project also depends on external providers, internal operational teams, compliance review, customer-support procedures, and user training.

A preliminary DFT-IRM assessment gives the following maturity profile:

$$m = (3, 2, 3, 1, 2)$$

This means that technology and data readiness are relatively advanced. The institution has documented the architecture, performed integration testing, addressed basic cybersecurity requirements, and mapped several external dependencies. Governance and strategy are also moderately developed: ownership is assigned, decision procedures exist, and the project is connected to a strategic objective.

However, operational resilience is only partly defined, people and adoption are incomplete, and risk and compliance are the weakest domain. Regulatory obligations have not yet been fully mapped into operational controls. Reporting procedures, outsourcing assessments, audit trails, and evidence for deployment approval are incomplete.

In this case, the formal readiness level is:

$$M = 1$$

because risk and compliance are critical for deployment and remain at Level 1. The progress index may be higher, but the organization should not proceed as if it were generally ready. The model therefore produces a practical recommendation: before deployment, the institution should prioritize compliance mapping, control documentation, regulatory reporting procedures, outsourcing assessments, and evidence that the service can be operated within the required legal and supervisory framework. This example illustrates the basic diagnostic role of DFT-IRM: it separates technical progress from responsible deployment readiness and makes the blocking domain visible.

4.3.2. AI-assisted transaction monitoring in a bank

A second example concerns a bank implementing an AI-assisted transaction-monitoring system for detecting suspicious payments, fraud signals, and unusual customer activity. This use case is more demanding because it combines financial data, machine-learning models, compliance obligations, operational workflows, human review, and auditability. Recent banking research likewise places AI adoption within questions of institutional resilience and financial stability (Siddik & Amin, 2026).

The system is trained on historical transaction data and connects to the bank's payment infrastructure, customer database, case-management system, and reporting workflow. Its purpose is not to automate final compliance decisions, but to prioritize alerts and support analysts in reviewing potentially suspicious activity.

A preliminary DFT-IRM assessment gives the following maturity profile:

$$m = (3, 2, 2, 2, 2)$$

Technology and data readiness are assessed at Level 3. The model has been developed, tested on historical data, integrated with internal systems, and documented at a technical level. Data pipelines exist, and basic cybersecurity controls are in place.

Operational resilience is assessed at Level 2. The system can run in a controlled environment, and monitoring procedures are partly defined. However, fallback procedures remain incomplete. It is not yet fully clear how analysts should proceed if the model becomes unavailable, produces abnormal alert volumes, or depends on delayed data feeds.

Governance and strategy are also assessed at Level 2. The project has management support and assigned owners, but decision rights are still incomplete. It is not fully clear who approves model changes, who accepts residual risk, who decides whether an alert threshold is appropriate, and who is accountable if the system changes analyst behavior.

Risk and compliance are assessed at Level 2. The organization has identified the regulatory relevance of the system and has begun translating it into controls. However, documentation of model assumptions, explainability limits, audit trails, reporting obligations, human-review requirements, and evidence for supervisory review is still incomplete.

People and adoption are assessed at Level 2. Some compliance analysts have been trained, but training is not yet systematic. There is a risk that staff either over-trust the system or ignore it when it conflicts with existing routines.

In this case, the formal readiness level is:

$$M = 2$$

The project is therefore more mature than the first example, but it is not yet ready for uncontrolled full deployment. There is no single acute failure point. Instead, several domains remain at the "Defined" level: procedures and partial controls exist, but the organization has not yet shown that the system is systematically monitored, tested, measured, and controlled in operation. The practical recommendation is not simply to improve model accuracy or add more technical sophistication. Instead, the bank should move from documentation to managed practice: tested fallback processes, threshold-change governance, audit-trail review, analyst training, monitoring of alert volumes, periodic model review, and evidence for internal and external supervision. Recent neuro-symbolic work illustrates one complementary technical pattern: separating learned interpretation from explicit symbolic verification of transaction constraints (Qin et al., 2026). This second example highlights a subtler use of DFT-IRM. A technically promising AI system may be more mature than an early-stage payment platform and still fall short of responsible full-scale operation. The model helps distinguish one critical blocking weakness from a broader need to move from defined procedures to managed capability.

5. Discussion: conventional finance and DeFi

DFT-IRM is designed primarily for conventional finance, including banking, payments, investment services, financial-market infrastructures, regulated fintech adoption, and technology modernization within financial institutions. In these settings, responsibilities are usually located within identifiable organizations. A bank, payment provider, investment firm, or infrastructure operator normally owns systems, employs operational teams, approves changes, maintains records, and answers supervisors.

The model can also be used to think about decentralized finance and related technologies. DeFi does not necessarily require a different maturity language, but it changes where responsibilities are located. Relevant capabilities may be distributed across protocol developers, smart contracts, validators or block producers, oracle providers, liquidity providers,

governance-token holders, interface operators, and users (Aramonte et al., 2021; Financial Stability Board, 2023; Schär, 2021; Werner et al., 2022). Earlier position work has likewise noted the need to adapt formal and symbolic methods to decentralized market settings (Žunić, 2022). Readiness is therefore still necessary, but it is harder to locate.

Technology readiness in DeFi must consider smart-contract risk, infrastructure dependency, oracle dependency, and protocol interaction. Operational resilience must consider network congestion, dependency on external protocols, limited emergency powers, and the difficulty of reversing erroneous actions. Governance readiness must examine who can change parameters, pause functions, coordinate responses, or communicate during incidents. Risk and compliance readiness must address uncertain legal responsibilities, cross-border activity, financial-crime exposure, and user protection. People and adoption must include the ability of users and operators to understand self-custody, transaction finality, permissions, and irreversible execution (Financial Stability Board, 2023; Werner et al., 2022).

This comparison should not be read as a claim that conventional finance is mature and DeFi is immature, or the reverse. Both environments require readiness; what differs is the location of responsibility. Conventional finance concentrates many responsibilities within regulated institutions, whereas DeFi distributes them across technical, economic, and governance layers (Aramonte et al., 2021; Schär, 2021). For process management, this distinction is important. Implementation readiness depends not only on technology, but also on where operational, legal, governance, and adoption capabilities reside in practice.

5.1. Limitations

DFT-IRM has clear limits:

First, the model is conceptual. It is informed by maturity-model literature, digital-transformation literature, operational-resilience guidance, and financial-technology risk literature, but it is not statistically validated (Becker et al., 2009; Pöppelbuß & Röglinger, 2011; Thordsen & Bick, 2023).

Second, the model is diagnostic rather than certifying. A high maturity assessment should not be interpreted as proof that technology is safe, profitable, legally compliant in every jurisdiction, or immune to failure.

Third, the progress index and the optional gap indicator should be used cautiously. Maturity levels are ordinal judgments supported by evidence, not exact physical measurements. These indicators may support comparison and prioritization, but they should not override the maturity profile or the bottleneck level. This caution is consistent with critical evaluations of digital maturity models (Thordsen & Bick, 2023; Thordsen et al., 2020).

Fourth, domain weights may vary by context. A retail payment system, an internal reporting platform, a cloud migration, and a DeFi interface may require different emphasis. The model provides a structure for assessment, but organizations must adapt the weighting and critical-domain selection to their own context.

Fifth, the model does not evaluate market mechanisms, trading rules, exchange-core computation, matching logic, Reaction Systems, concurrent exchange models, or the economic design of financial protocols. Those are separate research questions. DFT-IRM focuses only on organizational readiness for implementation and operation.

Different assessors may interpret the same evidence differently. Future empirical work should therefore examine inter-rater consistency and refine the assessment criteria where necessary. A further research challenge is to determine how DFT-IRM should distinguish the strength and coverage of different assurance techniques. Formal verification may establish selected properties under explicit assumptions, but its adoption requires specification effort, specialized expertise, suitable tools, and integration with the wider engineering process (Bowen

& Hinchey, 1995). Future work should examine how assurance techniques can be matched to system criticality, organizational capability, and regulatory expectations. These limitations define the model's intended use. DFT-IRM is meant to structure discussion, reveal gaps, and guide improvement before deployment.

6. Conclusion

Digital financial technology does not enter an organization in isolation. It becomes part of existing systems, data practices, regulatory obligations, operational routines, outsourcing arrangements, user habits, governance structures, and risk constraints. Implementation success therefore cannot be judged only by whether technology works.

This paper introduced DFT-IRM, the Digital Financial Technology Implementation Readiness Model. The model is maturity-based: it assesses readiness across five domains using five cumulative levels. These domains are technology and data readiness, operational resilience, governance and strategy, risk and compliance, and people and adoption. Readiness is reported through three connected outputs: a maturity profile, a bottleneck readiness level, and a progress index. The model's main contribution is to separate technical progress from responsible deployment readiness. A financial organization may have advanced software and still be unready because compliance controls are incomplete, recovery procedures are untested, responsibilities are unclear, or users are not prepared. At the same time, DFT-IRM can show where the organization is already strong and which domain most needs attention.

DFT-IRM is deliberately lightweight. It is neither a certification scheme nor a universal measurement scale, but a practical diagnostic framework for implementation planning, internal assessment, and process improvement. Although intended mainly for conventional financial organizations, it also clarifies readiness questions in decentralized finance, where responsibilities are more widely distributed. Future work should also examine how the model can distinguish between different strengths of technical evidence. Testing can expose defects in observed executions, whereas formal verification may establish selected properties of a formal model; deciding when such assurance is justified and organizationally feasible remains a demanding challenge. The central message is that financial organization is not ready merely because technology works. It is ready when the surrounding organization can operate, govern, monitor, recover, and adapt that technology responsibly.

Acknowledgments

OpenAI's ChatGPT was used only for language and readability improvement and formatting support. The authors reviewed the final manuscript and remained fully responsible for its content.

References

Al-Omoush, K. S., & Alsmadi, A. A. (2026). Determinants of FinTech adoption maturity and its impact on service innovation: Evidence from the banking sector. EuroMed Journal of Business. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/EMJB-08-2025-0307

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. BIS Quarterly Review, 21–36.

Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/publications/202103-guidelines-principles-operational-resilience.pdf (20.07.2026.)

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management: A procedure model and its application. Business & Information Systems Engineering, 1(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Bowen, J. P., & Hinchey, M. G. (1995). Ten commandments of formal methods. Computer, 28(4), 56–63. https://doi.org/10.1109/2.375178

Cervesato, I., Khan, S., Reis, G., & Žunić, D. (2019). Formalization of automated trading systems in a concurrent linear framework. Electronic Proceedings in Theoretical Computer Science, 292, 1–14. https://doi.org/10.4204/EPTCS.292.1

Committee on Payment and Settlement Systems, & Technical Committee of the International Organization of Securities Commissions (2012). Principles for financial market infrastructures. Bank for International Settlements. https://www.bis.org/publications/principles-financial-market-infrastructures.pdf (20.07.2026)

Dai, W., & Song, L. (2026). Bank digital transformation and market risk mitigation: A perspective from economic capital. International Journal of Finance & Economics, 31(1), 726–741. https://doi.org/10.1002/ijfe.3163

Dijkstra, E. W. (1972). Notes on structured programming. In O.-J. Dahl, E. W. Dijkstra, & C. A. R. Hoare (Eds.), Structured programming (pp. 1–82). Academic Press.

Financial Stability Board. (2023). The financial stability risks of decentralised finance. https://www.bis.org/publications/fsi-summary-financial-stability-risks-decentralised-finance-executive-summary.pdf (20.07.2026)

García-Llorente, C., & Olmeda, I. (2026). Algorithmic governance in banking: A comparative analysis of risk-based and accountability-oriented oversight. Journal of Banking Regulation, 27(2), 19. https://doi.org/10.1057/s41261-026-00320-6

Huynh, J. (2025). Digital transformation under the pressure of uncertainty in the banking sector. Economic Analysis and Policy, 86, 559–575. https://doi.org/10.1016/j.eap.2025.03.039

Ignatovich, D. A., & Passmore, G. O. (2015). Case study: 2015 SEC fine against UBS ATS. Aesthetic Integration Ltd.

Janulevičius, J. (2026). Zero-override architecture: Formally verified process flow integrity for security control enforcement in payment systems. Electronics, 15(17), 3905. https://doi.org/10.3390/electronics15173905

Papathomas, A., & Konteos, G. (2024). Financial institutions digital transformation: The stages of the journey and business metrics to follow. Journal of Financial Services Marketing, 29(2), 590–606. https://doi.org/10.1057/s41264-023-00223-x

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. In Proceedings of the 19th European Conference on Information Systems (Paper 28).

Qin, Y., Rhee, M., Teng, D., Zhang, C., & Zi, B. (2026). Neuro-symbolic constraint verification for LLM-driven internet finance transaction execution. Scientific Reports, ahead-of-print. https://doi.org/10.1038/s41598-026-65233-w

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153–174. https://doi.org/10.20955/r.103.153-74

Siddik, A. B., & Amin, N. U. (2026). Disruptive innovation or systemic resilience? Investigating the impact of artificial intelligence on banking stability. Research in International Business and Finance, 82, 103245. https://doi.org/10.1016/j.ribaf.2025.103245

Silva, R. P., Mamede, H. S., & Santos, V. (2025). A new proposed model to assess the digital organizational readiness to maximize the results of the digital transformation in SMEs. Journal of Innovation & Knowledge, 10(1), 100644. https://doi.org/10.1016/j.jik.2024.100644

Teichert, R. (2019). Digital transformation maturity: A systematic review of literature. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 67(6), 1673–1687. https://doi.org/10.11118/actaun201967061673

Thordsen, T., & Bick, M. (2023). A decade of digital maturity models: Much ado about nothing? Information Systems and e-Business Management, 21, 947–976. https://doi.org/10.1007/s10257-023-00656-w

Thordsen, T., Murawski, M., & Bick, M. (2020, April). How to measure digitalization? A critical evaluation of digital maturity models. In Conference on e-Business, e-Services and e-Society (pp. 358-369). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-44999-5_30

Wang, L., Zhao, X., & Wan, L. (2025). Analysis of the impact of bank digitization process on liquidity creation and risk-taking. Finance Research Letters, 79, 107234. https://doi.org/10.1016/j.frl.2025.107234

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2022). SoK: Decentralized finance (DeFi). In Proceedings of the 4th ACM Conference on Advances in Financial Technologies (pp. 30–46). ACM. https://doi.org/10.1145/3558535.3559780

Wing, J. M. (1990). A specifier's introduction to formal methods. Computer, 23(9), 8–24. https://doi.org/10.1109/2.58215

Yu, Z., & Liu, J. (2025). The digital revolution in banking: Unpacking risk management in the age of transformation. International Review of Economics & Finance, 103, 104444. https://doi.org/10.1016/j.iref.2025.104444

Zhang, Y., Zhao, L., & Li, C. (2025). Digital transformation and bank transparency: Evidence from China. Finance Research Letters, 86, 108520. https://doi.org/10.1016/j.frl.2025.108520

Žunić, D. D. (2022). Decentralized markets design and symbolic AI methods. In Proceedings of the 1st Serbian International Conference on Applied Artificial Intelligence (SICAAI), Kragujevac, Serbia, May 2022.

Žunić, D. D. (2023). A verifiable model of a minimal market operating sequentially, with price and time discrete. Journal of Computer and Forensic Sciences, 2(1), 7–17. https://doi.org/10.5937/jcfs2-44362

© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).