RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

The Agility Regulated Technology Transformation Framework: a risk-based methodology for technology governance, systems modernization, data security, and operational resilience in regulated financial institutions

O framework Agility de transformação tecnológica regulada: uma metodologia baseada em risco para governança de tecnologia, modernização de sistemas, segurança de dados e resiliência operacional em instituições financeiras reguladas

El framework Agility de transformación tecnológica regulada: una metodología basada en riesgos para la gobernanza tecnológica, la modernización de sistemas, la seguridad de los datos y la resiliencia operativa en instituciones financieras reguladas

Antonio Garcia Junior
Agility Digital Technologies, LLC., Florida, United States
Corresponding author: tony@agilitydigital.net
Short biography: Founder and owner of Agility Digital Technologies, LLC., with professional experience in financial-technology leadership, modernization, governance, architecture, data, risk, and operational resilience in regulated banking environments.

Abstract:
Financial institutions increasingly face the challenge of modernizing legacy technology environments while maintaining effective governance, cybersecurity, data protection, regulatory readiness, and operational resilience. Smaller and mid-sized banks, credit unions, fintech companies, payment organizations, and other regulated financial entities may face particular constraints because they must address complex technology and supervisory expectations with comparatively limited internal resources. This paper proposes the Agility Regulated Technology Transformation Framework (ARTTF), an internally developed, structured, and repeatable risk-based methodology designed to help regulated financial organizations assess technology maturity, identify material risks, prioritize remediation, and develop practical modernization roadmaps. The framework integrates six assessment domains: technology governance and executive accountability; legacy systems and technology architecture; data governance, identity, and access management; cloud, vendor, and third-party risk; cybersecurity, business continuity, and recovery; and auditability, regulatory readiness, and remediation governance. The methodology combines a five-level maturity model, a 30-question diagnostic instrument, qualitative risk prioritization, executive dashboard measures, and phased remediation planning. Its design draws on information-systems design science, digital-transformation literature, and recognized U.S. financial-sector and cybersecurity guidance, including NIST CSF 2.0 and FFIEC guidance. An illustrative community-bank scenario demonstrates how the framework can convert fragmented technology concerns into a prioritized governance and modernization program. The framework is intended as a practical management methodology and does not replace institution-specific legal, regulatory, audit, or supervisory requirements.

Keywords:
IT governance. Systems modernization. Data security. Operational resilience. Financial institutions.

Resumo:
Instituições financeiras enfrentam, de forma crescente, o desafio de modernizar ambientes tecnológicos legados ao mesmo tempo em que preservam governança efetiva, cibersegurança, proteção de dados, preparação regulatória e resiliência operacional. Bancos de pequeno e médio porte, cooperativas de crédito, fintechs, empresas de pagamentos e outras organizações

financeiras reguladas podem enfrentar restrições específicas, pois precisam responder a expectativas tecnológicas e de supervisão complexas com recursos internos comparativamente limitados. Este artigo propõe o Agility Regulated Technology Transformation Framework (ARTTF), uma metodologia baseada em risco, estruturada, repetível e desenvolvida internamente para apoiar organizações financeiras reguladas na avaliação da maturidade tecnológica, identificação de riscos materiais, priorização de remediações e desenvolvimento de roteiros práticos de modernização. O framework integra seis domínios: governança de tecnologia e responsabilidade executiva; sistemas legados e arquitetura tecnológica; governança de dados, identidade e controle de acesso; riscos de nuvem, fornecedores e terceiros; cibersegurança, continuidade de negócios e recuperação; e auditabilidade, preparação regulatória e governança de remediações. A metodologia combina modelo de maturidade de cinco níveis, instrumento diagnóstico com 30 perguntas, priorização qualitativa de riscos, indicadores para dashboard executivo e planejamento de remediação por fases. Seu desenho se baseia em design science de sistemas de informação, literatura de transformação digital e orientações reconhecidas do setor financeiro e de cibersegurança dos Estados Unidos. Um cenário ilustrativo de banco comunitário demonstra como o framework pode converter preocupações tecnológicas fragmentadas em um programa priorizado de governança e modernização, sem substituir requisitos legais, regulatórios, de auditoria ou de supervisão específicos de cada instituição.

Palavras-chave:
Governança de TI. Modernização de sistemas. Segurança de dados. Resiliência operacional. Instituições financeiras.

Resumen:
Las instituciones financieras afrontan cada vez más el desafío de modernizar entornos tecnológicos heredados mientras mantienen una gobernanza eficaz, ciberseguridad, protección de datos, preparación regulatoria y resiliencia operativa. Los bancos pequeños y medianos, cooperativas de crédito, empresas fintech, organizaciones de pagos y otras entidades financieras reguladas pueden enfrentar restricciones particulares porque deben responder a expectativas tecnológicas y de supervisión complejas con recursos internos comparativamente limitados. Este artículo propone el Agility Regulated Technology Transformation Framework (ARTTF), una metodología estructurada, repetible, basada en riesgos y desarrollada internamente para ayudar a las organizaciones financieras reguladas a evaluar la madurez tecnológica, identificar riesgos materiales, priorizar la remediación y desarrollar hojas de ruta prácticas de modernización. El framework integra seis dominios de evaluación: gobernanza tecnológica y responsabilidad ejecutiva; sistemas heredados y arquitectura tecnológica; gobernanza de datos, identidad y gestión de accesos; riesgo de nube, proveedores y terceros; ciberseguridad, continuidad del negocio y recuperación; y auditabilidad, preparación regulatoria y gobernanza de la remediación. La metodología combina un modelo de madurez de cinco niveles, un instrumento diagnóstico de 30 preguntas, priorización cualitativa de riesgos, medidas para un panel ejecutivo y planificación de remediación por fases. Su diseño se basa en la ciencia del diseño de sistemas de información, la literatura de transformación digital y orientaciones reconocidas del sector financiero y la ciberseguridad de Estados Unidos. Un escenario ilustrativo de banco comunitario demuestra cómo el framework puede convertir inquietudes tecnológicas fragmentadas en un programa priorizado de gobernanza y modernización, sin sustituir requisitos jurídicos, regulatorios, de auditoría o supervisión específicos de cada institución.

Palabras clave:

Gobernanza de TI. Modernización de sistemas. Seguridad de datos. Resiliencia operativa. Instituciones financieras.

1 Introduction

Technology modernization in financial services is not a purely technical exercise. It changes the way institutions deliver products, manage risk, protect data, interact with customers, depend on third parties, and demonstrate control effectiveness to boards, auditors, and supervisors. Digital-transformation research similarly emphasizes that meaningful transformation requires changes in organizational structures, processes, capabilities, and governance in addition to the adoption of new technologies (Vial, 2019). In regulated financial environments, this broader transformation challenge is intensified by requirements for safety and soundness, information security, resilience, data protection, third-party oversight, and auditable management accountability.

The challenge is especially visible in smaller and mid-sized financial institutions. Community banks and credit unions may operate critical payment, lending, deposit, and customer-information services while relying on comparatively small technology and risk teams. Fintech and payment companies may scale rapidly while becoming more dependent on cloud providers, banking partners, APIs, data platforms, and outsourced technology services. In both cases, modernization initiatives can create value only when the institution can identify which risks are material, establish clear ownership, sequence remediation, and preserve continuity during change.

U.S. financial-sector guidance increasingly treats technology governance, architecture, cybersecurity, operational resilience, authentication, and third-party management as interconnected management responsibilities. The FFIEC Architecture, Infrastructure, and Operations booklet emphasizes architecture and infrastructure planning, governance and risk management, and operational control across interconnected assets, processes, and third parties (Federal Financial Institutions Examination Council [FFIEC], 2021a). The FFIEC Business Continuity Management booklet frames continuity as an enterprise-wide risk-management discipline that encompasses technology, operations, testing, communication, and the resilience of critical services (FFIEC, 2019). Interagency third-party guidance further states that the use of third parties does not remove a banking organization's responsibility to operate safely, soundly, and in compliance with applicable requirements (Federal Deposit Insurance Corporation [FDIC] et al., 2023).

The need for a practical integration mechanism is therefore significant. Institutions often maintain separate inventories for audit findings, cybersecurity risks, architecture debt, data-quality issues, vendor concerns, disaster-recovery gaps, and regulatory actions. When these artifacts are managed in isolation, leaders may lack a consolidated view of how technology weaknesses interact or which actions should be prioritized first. A delayed identity-governance program, for example, can affect cybersecurity, audit readiness, third-party access, data protection, and incident containment simultaneously. An unsupported middleware platform can create operational, security, integration, and continuity risk at the same time.

This paper presents the Agility Regulated Technology Transformation Framework (ARTTF) as a practical method for converting these fragmented concerns into a structured transformation program. The framework is intended for community banks, small and mid-sized banks, credit unions, fintech companies, payment organizations, Banking-as-a-Service providers, and other regulated or data-intensive financial organizations. It is designed to support executive sponsors, technology leaders, risk and compliance professionals, internal audit stakeholders, program managers, and architecture teams in establishing a common fact base, evaluating maturity, prioritizing risk, and building an actionable roadmap.

The paper makes four practical contributions. First, it defines six integrated assessment domains that connect governance, architecture, data, third-party risk, cybersecurity, resilience, and regulatory readiness. Second, it provides a five-level maturity model and a 30-question diagnostic instrument that can be used for initial screening and executive discussion. Third, it defines a risk heat-map approach with explicit qualitative escalation rules so that simple scoring does not replace professional judgment. Fourth, it provides an executive dashboard model and a phased 0-90 day, 3-12 month, and 12-24 month roadmap structure to convert assessment findings into governed execution. An illustrative case demonstrates the mechanics of the approach without using confidential client data.

2 Theoretical and regulatory foundations

2.1 Digital transformation as an organizational and risk-management process

Digital transformation is commonly described as organizational change enabled by combinations of information, computing, communication, and connectivity technologies. Vial (2019) shows that digital transformation affects value creation while requiring organizations to address structural changes and barriers to execution. In a financial institution, these barriers

frequently appear as legacy applications, fragmented integration, unclear decision rights, inconsistent data ownership, vendor dependencies, manual controls, insufficient observability, or competing business and regulatory priorities.

This perspective is important because a modernization roadmap that focuses only on replacing technology can fail to address the operating model that created the risk. A core-system migration may leave unresolved data ownership, privileged-access weaknesses, vendor concentration, or ineffective change governance. Conversely, a governance initiative that does not address obsolete systems and architectural constraints may produce stronger documentation without reducing operational fragility. The ARTTF therefore treats technology transformation as a combined governance, architecture, data, security, resilience, and execution problem.

2.2 Governance, cybersecurity, and enterprise risk integration

NIST Cybersecurity Framework (CSF) 2.0 provides a high-level taxonomy that organizations of different sizes and maturity levels can use to understand, assess, prioritize, and communicate cybersecurity outcomes (Pascoe et al., 2024). Version 2.0 added the Govern function and increased emphasis on governance and supply-chain risk, reinforcing the need to connect cybersecurity to enterprise decision-making rather than treat it as an isolated technical program. NIST also emphasizes that the CSF describes outcomes rather than prescribing a single implementation method, which allows organizations to tailor implementation to their risk profile.

NIST's guidance on CSF Tiers can be used to characterize the rigor of cybersecurity risk governance and management processes and to provide context for improvement (Quinn et al., 2024). The ARTTF five-level maturity model is not a restatement of the four NIST CSF Tiers. It is an internally developed diagnostic scale intended to support broader technology-transformation assessment across six domains. NIST CSF outcomes and Tiers may be used as informative references within the cybersecurity-related portions of an assessment, while the ARTTF maturity score provides a cross-domain management view.

2.3 Architecture, legacy technology, and operational dependency

The FFIEC Architecture, Infrastructure, and Operations guidance recognizes that technology architecture, infrastructure, and operations are interconnected with assets, processes, and third-party service providers (FFIEC, 2021a). For regulated institutions, architecture decisions influence availability, security, scalability, vendor dependency, data

movement, change complexity, and the delivery of critical financial products and services. This makes architecture review a risk-management activity as well as a design activity.

Legacy technology should therefore be assessed not simply by age but by business criticality, supportability, security exposure, integration complexity, recoverability, knowledge concentration, change failure risk, and dependency on obsolete components. The framework uses these factors to identify modernization priorities and distinguish between technology that can be stabilized, technology that should be progressively decoupled, and technology that requires planned replacement.

2.4 Data governance, identity, and access management

Data governance determines which decisions must be made about data and who is accountable for making them. Khatri and Brown (2010) distinguish governance from day-to-day management and emphasize decision rights and accountability across data domains. In financial services, these governance questions are directly connected to reporting reliability, customer-data protection, fraud controls, model risk, analytics, AI readiness, and regulatory evidence.

Identity and access management is similarly cross-cutting. The FFIEC's 2021 authentication guidance emphasizes risk assessment, layered security, and stronger authentication practices for customers, employees, and third parties accessing systems and services (FFIEC, 2021b). For this reason, the framework evaluates access governance together with data classification, privileged access, segregation of duties, joiner-mover-leaver processes, and periodic entitlement review rather than treating authentication as an isolated control.

2.5 Cloud, vendor, and third-party risk

Modernization increasingly depends on external technology providers, cloud platforms, software-as-a-service products, fintech partners, and specialized vendors. The 2023 interagency third-party guidance establishes a risk-based life-cycle approach covering planning, due diligence and selection, contract negotiation, ongoing monitoring, and termination (FDIC et al., 2023). The guidance also makes clear that the banking organization retains responsibility for safe and sound operation when using third parties.

Cloud adoption creates additional considerations regarding shared responsibility, concentration, architecture transparency, exit planning, data location, identity, monitoring, resilience, and contractual access to evidence. U.S. Treasury and the Financial Services Sector

Coordinating Council have published resources intended to support secure cloud adoption and address third-party, outsourcing, resilience, and transparency concerns for financial institutions of different sizes (U.S. Department of the Treasury, 2024b). The ARTTF therefore embeds cloud and third-party governance into the same assessment used for architecture and operational resilience.

2.6 Cybersecurity, business continuity, and operational resilience

The concept of resilience extends beyond disaster recovery. FFIEC guidance emphasizes enterprise-wide continuity practices covering technology, business operations, testing, and communications, as well as continued maintenance of systems and controls needed to sustain critical services (FFIEC, 2019). The OCC's 2026 Cybersecurity and Financial System Resilience Report describes cybersecurity, operational resilience, and third-party risk as continuing supervisory priorities in the federal banking system (Office of the Comptroller of the Currency [OCC], 2026). The NCUA similarly highlights targeted examinations, risk assessments, preparedness, and system resilience in the credit-union sector (National Credit Union Administration [NCUA], 2026).

Within the ARTTF, resilience is evaluated through service criticality, recovery objectives, dependency mapping, backup and restore testing, incident readiness, crisis governance, monitoring, architecture redundancy, vendor recovery dependencies, and the organization's ability to sustain or restore critical financial services. This broader view reduces the risk that a technically successful backup program is mistaken for operational resilience.

2.7 Emerging technology and AI readiness

Advanced analytics and artificial intelligence can increase efficiency and decision support, but they also amplify the importance of data quality, explainability, security, third-party governance, and management accountability. NIST's AI Risk Management Framework provides a voluntary structure for managing risks to organizations and society arising from AI systems (Tabassi, 2023). Treasury's financial-sector work identifies data privacy, third-party dependencies, cybersecurity, bias, governance, and compliance as relevant considerations in financial-services AI adoption (U.S. Department of the Treasury, 2024a). The Financial Stability Board also identifies third-party dependencies, cyber risk, model risk, data quality, and governance among important AI-related vulnerabilities in finance (Financial Stability Board [FSB], 2024).

The ARTTF is not an AI governance framework. Instead, it treats AI readiness as an outcome of stronger foundational capabilities: accountable governance, reliable data, controlled access, secure architecture, effective third-party oversight, auditable change, and resilient operations. Institutions may extend the diagnostic instrument with AI-specific questions when advanced analytics or AI use cases are material to the scope.

3 Methodology

3.1 Applied design-science orientation

The framework was developed as a practice-oriented methodological artifact. Design science in information systems focuses on the creation and application of artifacts intended to improve human and organizational capabilities in a defined problem domain (Hevner et al., 2004). Peffers et al. (2007) describe a design-science research process that includes problem identification, definition of objectives, design and development, demonstration, evaluation, and communication. The development of the ARTTF follows this logic at an applied level: it identifies a recurring management problem in regulated technology transformation, specifies the capabilities needed to address it, designs a repeatable assessment and prioritization artifact, demonstrates its use through an illustrative case, and communicates limitations and opportunities for future empirical evaluation.

The methodology combines three knowledge sources. The first is recognized public guidance from U.S. financial regulators and standards bodies, used to identify recurring governance, architecture, cybersecurity, resilience, data, access, and third-party themes. The second is information-systems literature on digital transformation, data governance, and design science. The third is the author's professional experience in financial-technology leadership, modernization, governance, architecture, data, risk, and operational-resilience initiatives in regulated banking environments. The framework does not reproduce a regulator's examination program, scorecard, or proprietary control catalog. It translates recurring principles into a management-oriented sequence for assessment and transformation planning.

This paper does not claim empirical validation across a statistically representative sample of institutions. The illustrative case in Section 9 is hypothetical and is used only to demonstrate the mechanics of scoring, prioritization, executive reporting, and roadmap development. Future research should evaluate inter-rater consistency, predictive validity, and practical outcomes across different institution types and sizes.

3.2 Design principles

Table 1. Design principles of the Agility Regulated Technology Transformation Framework

Design principle	Operational meaning
Risk-based rather than checklist-driven	Assessment depth and remediation priority should reflect business criticality, regulatory relevance, customer/data impact, exposure, and operational dependency.
Executive accountability	Every material finding should have an accountable owner, decision path, target date, and escalation mechanism.
Evidence-oriented	Conclusions should be traceable to documents, interviews, inventories, configurations, metrics, testing evidence, or other review artifacts.
Cross-domain integration	A finding may affect multiple domains; the methodology should avoid siloed scoring that hides interconnected risk.
Proportionality	Assessment depth should reflect institution size, complexity, products, technology model, third-party dependency, and risk profile.
Modernization with resilience	Target-state changes should improve scalability and efficiency without weakening security, continuity, auditability, or control.
Actionability	The assessment should conclude with prioritized actions, sequencing, dependencies, owners, and executive decisions rather than a static list of observations.
Repeatability	Core domains, questions, scoring definitions, and reporting structures should be consistent enough to support reassessment and trend analysis.

Note. The principles are intended to guide professional judgment; they do not replace institution-specific supervisory or legal requirements.

3.3 Scope and intended use

The framework is designed for initial diagnostics, regulatory-readiness reviews, modernization assessments, governance improvement programs, due diligence, remediation planning, and transformation governance. It can be used as a complete enterprise assessment or scoped to a subset of domains, business units, platforms, or critical services. A complete assessment should establish scope boundaries, material systems and services, key third parties, critical data, regulatory context, and major transformation initiatives before scoring begins.

The intended users include CIOs, CTOs, CISOs, CROs, technology-risk leaders, compliance officers, data leaders, enterprise architects, program leaders, internal-audit stakeholders, and external advisors. The framework is not intended to create a certification, regulatory rating, or legal conclusion. A maturity score of 4 or 5 does not establish compliance, and a lower score does not by itself establish a regulatory violation. The score is a management tool for prioritization and dialogue.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

4 The Agility Regulated Technology Transformation Framework

4.1 Six-phase delivery lifecycle

Table 2. ARTTF six-phase lifecycle

Phase	Primary objective	Representative outputs
Phase 1 - Executive Alignment and Scope Confirmation	Define business context, regulatory drivers, scope, critical services, stakeholders, success criteria, timeline, and governance.	Engagement charter; scope statement; stakeholder map; document request list; initial risk hypotheses.
Phase 2 - Current-State Discovery and Evidence Collection	Review governance, architecture, applications, infrastructure, cloud, vendors, data, controls, continuity, audit findings, change practices, and reporting.	Current-state assessment; inventory; evidence register; dependency map; preliminary risk register.
Phase 3 - Risk-Based Gap and Maturity Assessment	Evaluate current practices against selected guidance, business requirements, risk appetite, and target outcomes; identify root causes and interconnected gaps.	Maturity scores; gap matrix; risk heat map; issue register; executive observations.
Phase 4 - Target-State Design and Modernization Roadmap	Translate findings into target operating models, governance, architecture, control improvements, sequencing, and investment priorities.	Target-state model; architecture blueprint; RACI; control plan; modernization roadmap; business-impact summary.
Phase 5 - Targeted Implementation Support	Provide governance and implementation support without operating as a staffing firm, MSP, penetration-testing provider, or continuous security-operations provider.	Implementation plan; governance dashboard; vendor tracker; issue/risk log; control evidence; updated procedures.
Phase 6 - Executive Reporting, Audit Evidence, and Continuous Improvement	Establish sustainable reporting, metrics, governance routines, evidence, reassessment, and lessons learned.	Executive report; board package; audit evidence; remediation dashboard; improvement backlog; reassessment baseline.

4.2 Six integrated assessment domains

Table 3. Integrated assessment domains

ID	Domain	Scope	Primary reference families
D1	Technology Governance and Executive Accountability	Decision rights, accountability, risk ownership, policies, governance forums, strategy alignment, executive/board reporting, risk appetite, and management oversight.	NIST CSF 2.0 Govern; FFIEC Management/AIO concepts; enterprise risk governance.
D2	Legacy Systems and Technology Architecture	Application and infrastructure lifecycle, target architecture, technical debt, integrations, APIs, cloud/on-premises dependencies, scalability, observability, change complexity, and modernization sequencing.	FFIEC Architecture, Infrastructure, and Operations; digital-transformation literature.
D3	Data Governance, Identity, and Access Management	Data ownership, classification, quality, lineage, access governance, privileged access, joiner-mover-leaver processes, segregation of duties, and reporting reliability.	Data-governance literature; FFIEC authentication/access guidance; NIST outcomes.
D4	Cloud, Vendor, and Third-Party Risk	Third-party inventory and tiering, due diligence, contracting, SLAs, ongoing monitoring, concentration, cloud shared responsibility, fourth parties, resilience, and exit planning.	2023 interagency third-party guidance; Treasury cloud resources; NIST supply-chain governance.
D5	Cybersecurity, Business Continuity, and Recovery	Security governance, vulnerability management, monitoring, incident response, backups, recovery testing, RTO/RPO, crisis management, critical-service continuity, and resilience dependencies.	NIST CSF 2.0; FFIEC Business Continuity Management; OCC and NCUA resilience priorities.

ID	Domain	Scope	Primary reference families
D6	Auditability, Regulatory Readiness, and Remediation Governance	Control mapping, evidence, audit/exam findings, regulatory-change tracking, policy adherence, issue ownership, remediation validation, reporting, and closure governance.	FFIEC/OCC supervisory themes; NIST governance; internal control and evidence practices.

4.3 Five-level maturity model

The maturity model provides a common language for describing the institutionalization of practices. It evaluates whether responsibilities and controls are informal or repeatable, whether they are documented and consistently executed, whether management measures performance and risk, and whether the organization has established continuous improvement and resilience. The scale is intentionally broad enough to apply across the six domains while allowing domain-specific evidence to determine the score.

A maturity score should be assigned only after reviewing evidence appropriate to the scope. Interview responses alone should not support a high score when documentation, operating evidence, testing, metrics, or issue history contradict the stated practice. Likewise, the absence of a formal document should not automatically force a low score if the organization can demonstrate an equivalent, controlled, and repeatable mechanism.

Table 4. ARTTF maturity scale

Level	Classification	Definition	Typical characteristics
1	Reactive	Practices are informal, fragmented, person-dependent, or primarily event-driven. Ownership and evidence are limited.	High variability; material gaps may be unknown; remediation is mainly reactive.
2	Developing	Basic controls and responsibilities exist, but execution is inconsistent across teams, systems, or periods.	Partial visibility; recurring exceptions; limited metrics; inconsistent evidence.
3	Defined	Practices are documented, assigned, standardized, and generally repeatable within the defined scope.	Roles and processes are clear; evidence is available; exceptions are managed.
4	Managed	Practices are measured, risk-based, monitored, and integrated into governance and management reporting.	Metrics, thresholds, testing, trend analysis, and accountable remediation are established.
5	Optimized / Resilient	Practices are integrated, adaptive, continuously improved, and demonstrably resilient under changing conditions.	Continuous learning; automation where appropriate; scenario testing; rapid response; strategic optimization.

Note. This five-level maturity model is an ARTTF diagnostic scale and should not be represented as equivalent to the NIST CSF four-Tier model.

4.4 Maturity scoring logic

Each diagnostic question is scored from 1 to 5 using the definitions in Table 4. A domain score is the arithmetic mean of the five questions assigned to that domain. The default

overall maturity score is the mean of the six domain scores. Equal weighting is suitable for an initial enterprise diagnostic because it avoids creating an appearance of precision before the institution has established its risk profile. Organizations may adopt risk-based weights when there is a documented rationale—for example, a payments organization may weight cyber resilience and third-party dependency more heavily, while an institution in a major core-modernization program may place greater emphasis on architecture and data.

The score should be accompanied by an evidence-confidence indicator such as High, Medium, or Low. A score based on policy documents, system evidence, metrics, test results, and issue history should carry greater confidence than a score based primarily on interviews. Where evidence is contradictory, the assessor should record the contradiction and use the lower supported score until the discrepancy is resolved.

5 30-question diagnostic instrument

5.1 Core questionnaire

The core diagnostic contains five questions for each of the six domains. The instrument is intended for structured interviews and evidence review, not as a self-certification checklist. Each question should be supported by a short evidence note, a maturity score from 1 to 5, and any resulting risk observation. The questions may be supplemented based on institutional products, regulatory perimeter, critical services, material vendors, and active transformation programs.

Table 5. ARTTF core 30-question diagnostic

No.	Domain	Diagnostic question	Score (1-5)
1	D1	Are technology strategy, risk priorities, and major modernization decisions governed through clearly defined executive forums with documented decision rights?	
2	D1	Are accountable owners formally assigned for material technology risks, controls, critical services, and remediation actions?	
3	D1	Are technology policies and standards subject to defined approval, exception, review, and retirement processes?	
4	D1	Are technology and cybersecurity risks integrated into enterprise risk management, risk appetite, and executive/board reporting?	
5	D1	Do management reports use decision-relevant KPIs/KRIs, thresholds, trends, and escalation criteria rather than activity metrics alone?	
6	D2	Does the institution maintain a reliable inventory of applications, infrastructure, integrations, critical dependencies, lifecycle status, and business ownership?	
7	D2	Are end-of-life, unsupported, high-complexity, or high-dependency technologies identified and governed through documented lifecycle and remediation plans?	
8	D2	Is there a documented target architecture and modernization roadmap aligned to business strategy, risk priorities, and critical-service resilience?	

No.	Domain	Diagnostic question	Score (1-5)
9	D2	Are integrations and APIs governed through defined architecture, security, data, versioning, ownership, and monitoring practices?	
10	D2	Are technical debt, change complexity, architecture exceptions, and modernization dependencies measured and incorporated into investment decisions?	
11	D3	Are data owners, data stewards, critical data elements, classification requirements, and accountability for data quality clearly defined?	
12	D3	Are data quality, lineage, reconciliation, and reporting issues measured, investigated, and remediated based on business and regulatory impact?	
13	D3	Are joiner-mover-leaver processes integrated with identity governance so that access is timely, traceable, and removed when no longer justified?	
14	D3	Are privileged and high-risk access rights subject to strong authentication, approval, logging, monitoring, and periodic recertification?	
15	D3	Are segregation-of-duties conflicts and access exceptions identified, risk-assessed, time-bound, and reviewed by accountable management?	
16	D4	Does the institution maintain a complete, risk-tiered inventory of third parties, cloud services, material subcontractors, and technology dependencies?	
17	D4	Does due diligence evaluate security, resilience, financial condition, data handling, regulatory support, concentration, and operational capabilities proportionate to risk?	
18	D4	Do contracts and SLAs address security, data rights, incident notification, audit/access rights, resilience, subcontracting, performance, termination, and exit needs?	
19	D4	Are material third parties subject to ongoing performance, risk, control, incident, and financial monitoring with defined escalation thresholds?	
20	D4	Are concentration risk, cloud shared-responsibility gaps, substitutability, data portability, and exit/transition plans evaluated for critical providers?	
21	D5	Are cybersecurity monitoring, logging, alerting, vulnerability management, and incident-escalation practices risk-based and effective for critical systems and services?	
22	D5	Is the incident-response program tested through exercises that include executive decision-making, communications, vendors, legal/compliance, and recovery coordination?	
23	D5	Are business impact analyses, RTOs, RPOs, recovery dependencies, and continuity plans current for critical financial products and services?	
24	D5	Are backup, restoration, failover, and disaster-recovery capabilities tested at a frequency and scope consistent with service criticality and threat scenarios?	
25	D5	Are significant resilience weaknesses, single points of failure, ransomware exposure, and recovery constraints tracked through accountable remediation?	
26	D6	Can material technology controls be mapped to documented evidence that demonstrates design, ownership, operation, testing, and exception handling?	
27	D6	Are audit, examination, compliance, and risk findings governed through a common issue-management process with owners, due dates, evidence, and validation?	
28	D6	Does the institution maintain a structured process for identifying applicable technology-related regulatory or supervisory changes and translating them into actions?	
29	D6	Are policies, procedures, standards, system evidence, testing results, and management approvals organized so they can be produced efficiently for audits or examinations?	
30	D6	Are overdue, recurring, or high-severity remediation items escalated to executive management and the board or appropriate committee with clear decisions and risk acceptance?	

5.2 Evidence expectations and scoring discipline

A diagnostic answer should be documented in four fields: score, evidence reviewed, observation, and action or risk reference. Typical evidence includes governance charters, board or committee materials, policies and standards, asset and application inventories, architecture diagrams, vendor records, contracts, access-review reports, vulnerability metrics, incident records, backup and recovery test results, audit findings, issue trackers, dashboards, and change records. The objective is not to maximize documentation volume; it is to establish traceability between the score and observable institutional practice.

Scores should describe institutionalization, not aspiration. A newly approved policy without operating evidence generally supports a Developing or Defined score depending on implementation scope; it should not automatically support Managed maturity. Conversely, a mature process may be supported by automated evidence and consistent operating history even if the organization uses a different terminology from the framework. Assessors should document compensating practices rather than force artificial conformity.

The questionnaire is deliberately concise. A full assessment should expand each question into sub-tests based on scope and materiality. For example, Question 24 may require separate review of immutable backup design, restoration testing, cyber-recovery isolation, critical-service failover, recovery dependencies, and vendor recovery evidence. The 30-question instrument is therefore best understood as an executive diagnostic and work-program organizer.

6 Risk assessment and prioritization model

6.1 Likelihood and impact scales

The risk model uses a 5 × 5 likelihood-impact matrix as a communication aid. Because qualitative risk matrices can create false precision, range compression, and ambiguous ordering, the numerical score should not be used as the sole basis for remediation decisions (Cox, 2008). The ARTTF therefore combines the base score with explicit escalation factors, service criticality, regulatory relevance, and professional judgment.

Table 6. Likelihood scale

Score	Level	Interpretation
1	Rare	Not expected under normal conditions; strong preventive controls and limited exposure.
2	Unlikely	Plausible but infrequent; exposure is limited or controls are generally effective.
3	Possible	Could occur under realistic conditions; known weaknesses or dependencies exist.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Score	Level	Interpretation
4	Likely	Expected to occur or recur without remediation; evidence of control weakness or repeated events.
5	Almost Certain	Active, recurring, highly exposed, or strongly evidenced as imminent/persistent.

Table 7. Impact scale

Score	Level	Interpretation
1	Limited	Localized effect; no material customer, regulatory, financial, or critical-service consequence.
2	Moderate	Manageable disruption or control failure with contained business impact.
3	Significant	Material operational, customer, data, audit, financial, or management impact requiring coordinated response.
4	Major	Serious impact to critical services, sensitive data, regulatory posture, financial loss, or sustained operations.
5	Severe / Critical	Potential for widespread or prolonged disruption, major customer/data harm, significant regulatory exposure, or threat to essential services.

6.2 Risk heat map and base priority bands

The base risk score is calculated as Likelihood × Impact, generating a value from 1 to 25. The default priority bands are Low (1-4), Moderate (5-9), High (10-14), and Critical (15-25). These bands are starting points and should be calibrated to the institution's risk appetite and issue-management policy. The matrix should not override mandatory remediation requirements, audit commitments, regulatory findings, or known critical vulnerabilities.

Figure 1. ARTTF risk heat map (base score)

Impact → Likelihood ↓	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Note. Base bands: Low = 1-4; Moderate = 5-9; High = 10-14; Critical = 15-25. Scores are a prioritization aid, not a quantitative estimate of expected loss.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

6.3 Qualitative escalation factors

Table 8. Risk-priority escalation factors

Escalation factor	Trigger	Treatment
Regulatory / supervisory significance	Finding relates to a regulatory commitment, examination finding, legal requirement, formal audit issue, or material supervisory expectation.	Elevate priority when delay could create regulatory, legal, or examination exposure.
Critical-service dependency	Finding affects payments, deposits, lending, customer access, identity, security, core processing, or another essential service.	Elevate when failure could impair a critical product/service or recovery dependency.
Sensitive-data / customer impact	Finding could materially expose confidential, customer, financial, authentication, or regulated data.	Elevate when data sensitivity, scale, or misuse potential is material.
External exposure / exploitability	Weakness is internet-facing, actively exploited, easily abused, or connected to weak credentials or privileged access.	Elevate based on threat intelligence, vulnerability evidence, or exposure.
Third-party concentration / substitutability	A critical provider has limited substitutes, opaque dependencies, inadequate exit capability, or concentration risk.	Elevate when institution has limited control or recovery alternatives.
Recovery fragility	Controls have not been tested, restoration is uncertain, RTO/RPO cannot be demonstrated, or single points of failure remain.	Elevate when failure could prolong disruption or make recovery uncertain.
Recurring / overdue issue	The same issue has repeated, exceeded target dates, or remained open through prior reviews.	Elevate to reflect ineffective remediation governance and accumulated exposure.

A recommended practice is to preserve the original base score and separately record the final management priority. For example, a base score of 12 may be designated Critical because it is an overdue regulatory finding affecting a critical payment service. This approach maintains scoring transparency and avoids manipulating likelihood or impact merely to achieve the desired priority.

7 Executive technology risk dashboard

7.1 Dashboard design

The executive dashboard translates assessment detail into a limited set of decision-relevant indicators. It should answer four questions: What is the current maturity and risk posture? Which risks require executive decisions? Is remediation progressing at the required pace? Are modernization initiatives improving or increasing resilience? The dashboard should therefore combine maturity, risk, remediation, resilience, architecture, third-party, and audit indicators rather than reporting cybersecurity activity alone.

Metrics should be defined with an owner, calculation logic, data source, threshold, frequency, and escalation path. A dashboard without thresholds can become a reporting artifact rather than a management control. Equally, an excessive number of metrics can hide

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

the few issues that require action. The ARTTF recommends a compact executive view supported by deeper operational drill-downs.

Table 9. Recommended executive dashboard measures

Indicator	Definition	Frequency	Executive use
Overall technology maturity	Average domain maturity score plus evidence-confidence level.	Quarterly	Trend and target by assessment cycle.
Domain maturity	D1-D6 maturity scores.	Quarterly	Highlight domains below target or declining.
Critical / High technology risks	Count and trend of open Critical and High items.	Monthly	Escalate new Critical items immediately.
Overdue remediation	Number and percentage of issues beyond approved target date.	Monthly	Escalate material overdue items and repeat extensions.
Regulatory / audit findings	Open findings by severity, age, due date, and validation status.	Monthly	Separate commitments requiring formal closure evidence.
Critical legacy exposure	Critical services dependent on unsupported/high-risk technology.	Quarterly	Track retirement, containment, and decoupling milestones.
High-risk third parties	Material providers with open control, performance, resilience, or contract issues.	Monthly	Include concentration and exit-plan status.
Privileged-access exceptions	High-risk accounts/exceptions outside policy or recertification requirements.	Monthly	Escalate unowned, stale, shared, or excessive privilege.
Patch / vulnerability SLA compliance	Percentage of material vulnerabilities remediated within defined risk-based SLA.	Monthly	Segment by exposure and business criticality.
Backup / recovery test success	Critical services with successful, evidenced restore/failover tests.	Quarterly	Track failed tests and unproven recovery dependencies.
Incident / crisis exercise readiness	Status and closure of lessons from tabletop or recovery exercises.	Quarterly / Semiannual	Escalate unresolved high-impact exercise findings.
Remediation closure rate	Items closed and independently validated versus opened during period.	Monthly	Monitor backlog growth and recurrence.
Modernization milestone health	Critical roadmap milestones on track, at risk, or delayed.	Monthly	Link delays to risk exposure and executive decisions.
Executive decisions required	Open funding, risk-acceptance, sequencing, vendor, or scope decisions.	Monthly	Keep decision log with owner and due date.

7.2 Governance cadence

A practical governance cadence combines monthly remediation and transformation reviews, quarterly executive risk reviews, and periodic board or board-committee reporting based on the institution's governance model. Critical risks should not wait for a scheduled meeting. The dashboard should preserve decision history, approved risk acceptance, target-date changes, and the rationale for material sequencing decisions. This creates an auditable link between assessment findings and executive accountability.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

8 Remediation and modernization roadmap

8.1 Roadmap principles

The roadmap converts risk and maturity findings into sequenced action. The order should not be determined only by the highest numerical risk score. Some actions are prerequisites for others: an institution may need to establish application ownership and dependency mapping before it can safely rationalize applications; it may need to stabilize backup recovery before beginning a high-risk infrastructure migration; and it may need data ownership and classification before implementing advanced analytics at scale.

For this reason, the ARTTF uses three planning horizons. The first 0-90 days emphasizes governance, evidence, urgent exposure reduction, and quick wins. The 3-12 month horizon institutionalizes controls and executes medium-complexity modernization. The 12-24 month horizon addresses structural transformation, major platform changes, data architecture, resilience engineering, and continuous improvement. Timing should be adapted to the institution's risk profile, resource capacity, vendor constraints, and regulatory commitments.

Table 10. Phased remediation and modernization roadmap

Horizon	Priority actions	Representative deliverables	Expected management outcome
0-90 days - Stabilize and establish control	Confirm executive governance and accountable owners; validate critical-service and technology inventories; identify unsupported critical assets; close urgent privileged-access and authentication gaps; validate backup/restoration for critical services; tier material vendors; create unified issue register; establish regulatory/audit closure plan; define target-state decision principles.	Governance charter; owners/RACI; critical inventory; top-risk register; validated quick wins; executive dashboard baseline; 90-day remediation plan.	Unknown or unowned risk becomes visible; immediate exposure is contained; executives have a common fact base.
3-12 months - Institutionalize and modernize	Implement target architecture and modernization waves; formalize data governance; strengthen IAM/PAM and access recertification; improve vulnerability and observability practices; establish cloud and vendor governance; test BCP/DR and incident response; improve policy lifecycle; automate evidence where practical; execute high-priority remediation.	Target architecture; modernization backlog; data governance operating model; vendor monitoring; tested recovery evidence; improved controls; measurable remediation trend.	Controls become repeatable and measurable; critical technical debt and resilience gaps begin to decline.
12-24 months - Transform and optimize	Execute major legacy/core modernization; decouple integrations and strengthen API/platform architecture; modernize data architecture; implement resilience engineering and dependency testing; optimize cloud operating model; automate governance and reporting; prepare advanced analytics/AI use cases on controlled foundations; embed continuous reassessment.	Modernized platforms; resilient architecture; improved data foundations; continuous metrics; optimized governance; reassessment showing maturity improvement.	Structural risk is reduced; modernization and resilience reinforce one another; continuous improvement is institutionalized.

8.2 Prioritization and sequencing rules

1. Address immediate safety, customer, regulatory, and critical-service exposures before optimization work.

2. Establish ownership and evidence before relying on maturity scores for investment decisions.

3. Resolve foundational identity, recovery, inventory, and dependency gaps that could undermine later modernization.

4. Sequence modernization by business capability and dependency rather than application age alone.

5. Use containment when immediate replacement is impractical, but define an explicit exit or modernization milestone.

6. Treat vendor and cloud dependencies as part of the service architecture, including recovery and exit planning.

7. Integrate audit and regulatory commitments into the same roadmap used for technology transformation.

8. Require executive decisions for accepted risk, repeated deadline extensions, material scope reductions, and changes that affect critical services.

9. Reassess maturity and residual risk after material remediation or major modernization waves.

10. Preserve traceability from finding to risk, action, evidence, validation, and closure.

9 Illustrative application

9.1 Hypothetical institution and scope

The following case is fictional and is provided solely to demonstrate the mechanics of the framework. It does not represent an actual client, financial institution, assessment, or regulatory conclusion.

HarborView Community Bank (HCB) is modeled as a hypothetical regional community bank with approximately $3 billion in assets, a mixed branch/digital operating

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

model, several hundred employees, and material dependence on a core banking provider, cloud-hosted customer applications, payment vendors, and outsourced technology services. Management plans a multi-year digital modernization program but has accumulated open audit issues, point-to-point integrations, inconsistent data ownership, and several high-dependency vendor relationships. The assessment scope covers the six ARTTF domains and focuses on critical deposit, payment, digital-channel, customer-information, and financial-reporting services.

9.2 Illustrative maturity results

Table 11. Illustrative maturity results for HCB

Domain	Description	Score	Illustrative interpretation
D1	Technology Governance and Executive Accountability	2.8	Defined governance forums exist, but ownership and KRI thresholds are inconsistent.
D2	Legacy Systems and Technology Architecture	1.8	Several critical components are aging; target architecture and dependency mapping are incomplete.
D3	Data Governance, Identity, and Access Management	2.2	Access controls exist, but data ownership, privileged-access governance, and recertification need strengthening.
D4	Cloud, Vendor, and Third-Party Risk	2.0	Material vendors are known, but concentration, exit planning, and ongoing monitoring are inconsistent.
D5	Cybersecurity, Business Continuity, and Recovery	2.4	Security operations are established, but recovery evidence and cross-vendor resilience testing are incomplete.
D6	Auditability, Regulatory Readiness, and Remediation Governance	2.6	Issue tracking exists, but overdue findings and evidence quality require stronger executive governance.
Overall	Equal-weighted maturity	2.3	Overall classification: Developing.

The illustrative overall score of 2.3 indicates that HCB has established several foundational practices but lacks consistent institutionalization across architecture, third-party governance, data/access management, and recovery. The most important observation is not the average itself; it is the uneven maturity profile. A bank can maintain relatively mature cybersecurity operations while still carrying material risk through unsupported technology, weak vendor exit planning, or unproven recovery dependencies.

9.3 Illustrative priority risks

Table 12. Illustrative risk register and prioritization

ID	Risk	L	I	Base / final priority	Escalation rationale	Immediate treatment
R1	Unsupported middleware supporting critical payment integrations	4	5	20 - Critical	Externally connected dependency, limited internal expertise, critical payment service.	Contain exposure; confirm vendor/support options; accelerate decoupling/replacement plan.

ID	Risk	L	I	Base / final priority	Escalation rationale	Immediate treatment
R2	Privileged accounts with incomplete recertification and inconsistent ownership	4	4	16 - Critical	High privilege and sensitive-system access; audit relevance.	Emergency recertification; remove stale access; implement PAM governance and monitoring.
R3	Critical-service restoration has not been demonstrated end-to-end across key vendors	3	5	15 - Critical	Recovery fragility and third-party dependency.	Execute restore/failover test; validate RTO/RPO and vendor dependencies; close evidence gaps.
R4	Material cloud provider agreement lacks sufficiently detailed exit/transition provisions	3	4	12 - High	Concentration and substitutability concerns.	Perform contract and exit-plan review; define data portability and transition requirements.
R5	High-severity audit finding has exceeded target date after two extensions	3	4	12 - Critical (escalated)	Recurring/overdue governance factor and audit commitment.	Executive escalation; recovery plan; independent validation before closure.
R6	Critical data elements lack formally assigned owners and quality thresholds	3	3	9 - Moderate	Impacts reporting reliability and modernization/analytics readiness.	Establish ownership and data-quality operating model in 3-12 month horizon.

9.4 Illustrative executive dashboard snapshot

Table 13. Illustrative executive dashboard

Indicator	Current state	Target	Status	Executive comment
Overall maturity	2.3 - Developing	Target 3.0 within 12 months	Amber	Architecture and TPRM are the lowest domains.
Critical risks	4	Target ≤ 1 within 90 days	Red	R1, R2, R3, R5 require executive tracking.
High risks	1	Declining trend	Amber	R4 cloud exit risk.
Overdue remediation	7 items; 2 material	No material overdue items	Red	R5 requires recovery plan and governance action.
Critical legacy exposure	3 critical services	All with funded modernization/containment plan	Red	Payment middleware is top priority.
High-risk third parties	6; 2 with open issues	All with active monitoring and exit posture	Amber	Contract and concentration review required.
Privileged-access exceptions	14	Zero unowned/stale high-risk exceptions	Red	Immediate recertification in progress.
Recovery testing	3 of 5 critical services end-to-end tested	5 of 5	Amber	Cross-vendor restoration must be completed.
Modernization milestones	2 at risk	No critical milestone without executive decision	Amber	Dependency mapping delays architecture sequencing.

9.5 Illustrative roadmap

In the first 90 days, HCB would establish a single executive remediation forum, validate the critical-service/application/vendor inventory, complete privileged-access recertification, perform an end-to-end recovery test for the highest-criticality services, establish a recovery plan for overdue audit issues, and define containment and replacement

milestones for unsupported payment middleware. These actions would reduce immediate exposure while improving the evidence base for longer-term modernization.

During months 3-12, HCB would execute the first architecture-modernization wave, formalize data ownership and quality thresholds, improve privileged-access management, strengthen cloud and vendor monitoring, complete critical-service BCP/DR testing, and rationalize issue-management and control-evidence processes. The objective would be to reach a Defined level across all domains and establish Managed practices for the highest-risk areas.

During months 12-24, HCB would continue decoupling legacy integrations, implement target-state platform and data architecture, improve resilience engineering and dependency testing, automate selected evidence and risk reporting, and establish an operating model for responsible analytics and AI readiness. A formal reassessment would compare domain maturity, residual risk, overdue issues, recovery evidence, and modernization outcomes against the original baseline.

10 Discussion

The central proposition of the ARTTF is that technology risk and technology modernization should be managed through a common executive lens. Financial institutions often organize responsibilities by specialized functions—cybersecurity, infrastructure, architecture, data, vendor management, compliance, internal audit, and program delivery. Specialization is necessary, but it can fragment accountability when the institution must decide which transformation actions matter most. The framework creates a shared vocabulary without requiring these functions to collapse into a single team.

A second contribution is the explicit separation of maturity and risk. Maturity asks how consistently and effectively a capability is institutionalized. Risk asks what could happen, how likely it is, how severe the impact may be, and what additional context changes priority. A low maturity score may not create immediate high risk when the process supports a low-criticality service with limited exposure. Conversely, a generally mature organization may still have a single critical vulnerability or untested recovery dependency that requires immediate action. Treating maturity and risk as separate but connected concepts helps avoid simplistic interpretations.

A third contribution is the use of evidence confidence. Technology assessments frequently depend on interviews with leaders who understand intended processes but may not

see local exceptions. Recording evidence confidence makes uncertainty visible and directs follow-up testing. It also supports more credible reassessment because improvements can be evaluated through operating evidence rather than changes in perception alone.

The framework also emphasizes the relationship between modernization and operational resilience. Modernization can reduce risk by eliminating unsupported systems, reducing manual processes, improving observability, strengthening identity, and simplifying integrations. It can also increase risk when migration introduces new dependencies, weakens recovery design, creates concentration, or changes operating responsibilities faster than governance can adapt. A risk-based roadmap therefore treats resilience as a design requirement for modernization, not a post-implementation control.

For small and mid-sized institutions, proportionality is particularly important. The objective is not to replicate the staffing, documentation, or tooling model of a large global bank. It is to demonstrate that governance and controls are appropriate to the institution's size, complexity, products, data, technology dependency, and risk profile. The same diagnostic question may therefore lead to different evidence expectations in a community bank, a fintech platform, and a large payment company.

The framework can also support knowledge transfer. Because the domains, questions, scoring definitions, heat-map approach, dashboard measures, and roadmap horizons are documented, internal teams can reuse the method during periodic reassessment, project governance, vendor reviews, and executive planning. This repeatability can reduce dependence on one-time assessments and help institutions build internal technology-risk management capability.

11 Limitations and future research

The ARTTF has several limitations. First, the current paper presents a conceptual and applied methodology rather than an empirically validated predictive model. The five-level scale and diagnostic questions have not yet been tested for statistical reliability across a representative population of financial institutions. Second, qualitative risk scoring depends on assessor judgment. Although evidence requirements and escalation factors reduce subjectivity, different assessors may still reach different scores. Third, institution-specific legal and regulatory obligations vary by charter, regulator, product, geography, data, and activity; a generalized framework cannot replace tailored legal, compliance, or supervisory analysis.

Fourth, the framework deliberately uses a compact set of 30 questions. This supports executive usability but means that a complete engagement must expand the questions into detailed procedures and evidence tests. Fifth, technology risk changes rapidly. Threat conditions, regulatory expectations, cloud architectures, AI use cases, vendor dependencies, and products evolve, so diagnostic criteria should be periodically reviewed and version-controlled.

Future research should evaluate the framework through multiple case studies across community banks, credit unions, fintech companies, and payment organizations. Useful research questions include inter-rater consistency, the relationship between maturity improvements and issue closure, the effect of evidence confidence on scoring accuracy, the value of different domain weights, and whether roadmap sequencing improves remediation cycle time or reduces recurring findings. Future work could also develop sector-specific extensions for payment processing, Banking-as-a-Service, wealth management, and responsible AI adoption.

12 Final considerations

Regulated financial organizations must modernize while preserving control, security, auditability, and continuity. These objectives are often managed through separate programs even though the underlying technology dependencies are shared. The Agility Regulated Technology Transformation Framework provides an integrated method for connecting those concerns through six domains, a five-level maturity model, a 30-question diagnostic, risk prioritization, executive reporting, and phased transformation planning.

The framework is intentionally practical. It begins with executive alignment and evidence, distinguishes maturity from risk, and concludes with a roadmap that assigns ownership and sequencing. The illustrative case shows how an institution can move from fragmented observations to a consolidated view of technology risk and modernization priorities. The most important output is not a numerical maturity score; it is a defensible management narrative that explains what is material, why it matters, who owns it, what evidence supports the conclusion, and what action should occur next.

Used appropriately, the methodology can support regulatory readiness, audit remediation, systems modernization, data and access governance, third-party oversight, cybersecurity, and operational resilience. It is designed to complement—not replace—recognized frameworks and supervisory guidance. Its value lies in translating those principles

into a repeatable executive process for prioritizing and governing technology transformation in regulated financial environments.

13 Declarations

Conflict of interest: The author is the founder and owner of Agility Digital Technologies, LLC., and developed the framework described in this paper. This affiliation is disclosed because the framework bears the company name.

Funding: No external funding was received for the preparation of this methodological paper.

Ethics statement: This paper does not involve human subjects, animal subjects, or confidential client data. The illustrative case is entirely hypothetical.

Data availability: No empirical dataset was created or analyzed. All case data and scores presented for demonstration are hypothetical.

14 References

Cox, L. A., Jr. (2008). What's wrong with risk matrices? Risk Analysis, 28(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, & Office of the Comptroller of the Currency. (2023). Interagency guidance on third-party relationships: Risk management. https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

Federal Financial Institutions Examination Council. (2019). Business Continuity Management booklet. FFIEC Information Technology Examination Handbook. https://www.ffiec.gov/news/press-releases/2019/pr-11-14

Federal Financial Institutions Examination Council. (2021a). Architecture, Infrastructure, and Operations booklet. FFIEC Information Technology Examination Handbook. https://www.ffiec.gov/news/press-releases/2021/pr-06-30

Federal Financial Institutions Examination Council. (2021b). Authentication and Access to Financial Institution Services and Systems guidance. https://www.ffiec.gov/news/press-releases/2021/pr-08-11

Financial Stability Board. (2024). The financial stability implications of artificial intelligence. https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105. https://aisel.aisnet.org/misq/vol28/iss1/6/

Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152. https://doi.org/10.1145/1629175.1629210

National Credit Union Administration. (2026). 2025 cybersecurity and credit union system resilience report. https://ncua.gov/news/publication-search/cybersecurity/2025-cybersecurity-and-credit-union-system-resilience-report

Office of the Comptroller of the Currency. (2026). 2026 cybersecurity and financial system resilience report. https://www.occ.treas.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/index-cybersecurity-and-financial-system-resilience-report.html

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick-start guide for using the CSF Tiers (NIST SP 1302). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1302

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

U.S. Department of the Treasury. (2024a, December 19). Treasury releases report on the uses, opportunities, and risks of artificial intelligence in financial services. https://home.treasury.gov/news/press-releases/jy2760

U.S. Department of the Treasury. (2024b, July 17). Treasury and the Financial Services Sector Coordinating Council publish new resources on effective practices for secure cloud adoption. https://home.treasury.gov/news/press-releases/jy2467

U.S. Department of the Treasury. (2026, February 19). Treasury releases two new resources to guide AI use in the financial sector. https://home.treasury.gov/news/press-releases/sb0401

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