ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

Development and Validation of the R-DAIR Maturity Framework for Continuous Revenue Data Integrity Assessment and Revenue Leakage Prevention in Small and Community Financial Institutions

Adetoun Adeleke
Georgia State University, Robinson College of Business,
Atlanta, Georgia

Abstract
Small and community financial institutions increasingly rely on interconnected transaction, payment, lending, accounting, and reporting systems while revenue controls often remain periodic. This study develops and validates the Open Revenue Data Assurance, Integrity & Reliability (R-DAIR) Maturity Framework as the empirical core of an openly deployable, vendor-neutral standard for continuous revenue-data integrity assessment and leakage prevention. The study combined framework design, expert content validation, pilot testing, survey-based maturity assessment, and operational validation across 30 institutions, 240 main respondents, 12 experts, 40 pilot respondents, and 360 institution-month records. Ten validated subdimensions were organized beneath four public-facing domains: Data Quality & Record Integrity, Anomaly Detection & Revenue Assurance, Workflow & Systems Integration, and Workforce Capability. Average relevance and clarity I-CVIs were 0.94 and 0.92. Cronbach alpha ranged from 0.84 to 0.91, composite reliability from 0.87 to 0.93, and AVE from 0.55 to 0.68. Model fit was good (CFI=0.955, TLI=0.947, RMSEA=0.049, SRMR=0.043). The mean maturity score was 2.99. Higher maturity was positively associated with reconciliation completeness (r=0.750), recovery (r=0.788), and automation (r=0.804), and negatively associated with revenue leakage (r=-0.743), detection latency (r=-0.814), unresolved exceptions (r=-0.740), and recurrence (r=-0.745), all $p<0.001$. The results support R-DAIR as a measurable pathway from periodic checking to continuous, preventive revenue assurance suitable for smaller institutions and extensible to SMEs.

Keywords:
Continuous Monitoring, Data Integrity, Maturity Model, Open Standard, Revenue Assurance, Revenue Leakage, Small Financial Institutions.

I. Introduction

A. Background and Problem Context

Revenue operations depend on trustworthy records. Interest income, transaction fees, service charges, loan-related income, renewals, settlements, and accounting adjustments may originate in different applications before reaching subledgers, the general ledger, management reports, and financial statements. A defect at any point can affect completeness, accuracy, consistency, timeliness, or traceability. The exposure is acute in smaller institutions that combine core applications with vendor platforms, spreadsheets, batch interfaces, and limited specialist staffing. Revenue-data integrity is therefore simultaneously an information-quality, governance, operational-risk, technology, and internal-control problem.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

The information-quality literature establishes that dependable data cannot be reduced to accuracy alone. Wang and Strong identified intrinsic, contextual, representational, and accessibility dimensions [1]; Lee et al. operationalized those dimensions through AIMQ [2]; and Pipino et al. showed the value of combining subjective and objective quality assessment [3]. In banking, the BCBS principles similarly emphasize governance, architecture, accuracy, completeness, timeliness, and adaptability [4]. These concepts matter directly to revenue assurance because a transaction may be numerically correct at source yet still be unfit for assurance if it is incomplete, late, inconsistently mapped, or untraceable across systems.

Revenue leakage is the monetary consequence of failed data, process, configuration, or control logic. Omitted fees, incorrect pricing or interest calculations, failed postings, incomplete settlements, duplicate reversals, unauthorized overrides, and unresolved suspense items can all produce foregone or incorrectly recognized revenue. Periodic reconciliation and audit remain necessary, but the interval between reviews can allow defects to persist. Continuous-auditing research shows how automation and exception-oriented procedures can increase assurance frequency [5], [6]. In a financial setting, Olaseinde's real-time detection work further emphasizes the importance of reducing detection latency when transaction velocity is high [7].

B. Alignment with the Proposed Open R-DAIR Standard

R-DAIR is framed as the Open Revenue Data Assurance, Integrity & Reliability Standard: an openly deployable, vendor-neutral maturity framework intended to support self-administered assessment, continuous integrity scoring, anomaly detection, exception routing, remediation planning, and practitioner training. The research reported here supplies the measurement and validation layer of that wider endeavor. The empirical model contains ten subdimensions, but the public standard organizes them into four higher-order domains so that the instrument remains understandable to SMEs, credit unions, cooperatives, and community financial institutions without requiring specialist data-science staff.

The intended value proposition is not artificial intelligence itself. Advanced analytics may assist anomaly prioritization at higher maturity levels, but the standard remains useful when controls are rule-based, reconciliations are automated, and alerts are handled by accountable owners. This distinction is important because smaller institutions must be able to improve integrity even when they cannot deploy sophisticated models. The present paper therefore evaluates maturity as an integrated governance and control capability rather than as a technology score.

C. Aim and Contribution

The study aimed to develop and validate R-DAIR, classify participating institutions across five maturity levels, and test whether higher maturity corresponds with stronger operational outcomes. Seven directional hypotheses examined revenue leakage, reconciliation completeness, detection latency, unresolved exceptions, revenue recovery, leakage recurrence, and maturity-level performance differentiation. The contribution is both academic and practical: it links a maturity construct to measurable revenue outcomes and provides a defensible empirical foundation for an open standard and self-assessment toolkit.

II. Literature Review and Related Standards

A. Data Governance, Quality, and Assurance

Revenue integrity requires both technical controls and accountable governance. Khatri and Brown argue that data governance depends on explicit decision rights and responsibilities [8], while COSO connects risk assessment, control activities, information, monitoring, and accountability within an integrated control system [9]. Ashimolowo and Oginni similarly associate governance discipline with performance stability and strategic assurance in high-risk settings [10]. Although their context differs from financial revenue operations, the governance principle transfers directly: automated controls cannot compensate for unclear ownership, inconsistent definitions, or weak escalation responsibility.

Accounting systems increasingly operate within broader enterprise data ecosystems, making provenance and interface control central to dependable reporting [20]. For smaller institutions, fragmentation can arise even without large scale because several outsourced platforms, manual files, and specialized applications may coexist. End-to-end reconciliation therefore becomes a population-

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

level control that tests whether source activity, settlement records, subledgers, and ledger postings agree. R-DAIR treats reconciliation completeness, data ownership, lineage, and auditability as foundational capabilities rather than isolated checks.

B. Continuous Monitoring and Data-Driven Assurance

Continuous monitoring repeatedly executes controls using system-generated evidence and routes deviations for investigation. Relevant methods include automated matching, validation rules, duplicate detection, threshold alerts, trend analysis, exception dashboards, and anomaly detection. Alles et al. show how continuous auditing shifts assurance from periodic inspection toward automated, exception-focused processes [5], [6]. Data-driven monitoring studies in other resource-constrained domains also illustrate a transferable design principle: continuous observation can be combined with structured modelling even when data are fragmented or limited. Adeyekun, Orekoya, and Abiola demonstrate this logic in climate-resilience monitoring [11], while Adeyekun extends it toward predictive risk assessment in a data-limited environmental setting [12]. R-DAIR applies the same general logic to revenue records, where accumulated exception history can support progressively more anticipatory control.

AI can assist pattern recognition, but it also introduces reliability concerns when users treat opaque outputs as control evidence. Olaseinde and Azeez caution against uncritical auditor reliance on hallucinating generative-AI models [13]. This reinforces a core R-DAIR principle: AI may be used inside the scoring or detection engine, but every alert, override, and remediation decision should remain traceable to validated data, explicit rules, and accountable review. The standard is therefore designed to remain valuable independent of any particular AI technology cycle.

C. Maturity Models and Composite Scoring

Maturity models organize capability into ordered stages that support diagnosis and improvement. de Bruin et al. describe development phases covering scope, design, population, testing, deployment, and maintenance [14]. Becker et al. emphasize theoretical grounding and transparent construction [15], while Pöppelbuß and Röglinger stress clear application domains, verifiable criteria, and prescriptive improvement paths [16]. R-DAIR follows these principles through a specific revenue-assurance domain, explicit subdimensions, bounded score ranges, defined operating states, and empirical validation against operational outcomes.

Composite scoring is appropriate where performance depends on several interdependent capabilities. Ashimolowo's weighted composite model for risk-based quality governance provides a related example of aggregating multiple criteria into an interpretable decision score while retaining diagnostic meaning at the component level [17]. R-DAIR similarly aggregates dimension scores into an institutional maturity value but preserves subdimension scores for remediation prioritization.

D. Related Standards and Research Gap

ISO 8000-61 provides a process reference model for data-quality management [18], and DCAM provides a broad enterprise data-management capability framework [19]. These approaches are useful reference points but do not directly provide a revenue-specific, self-administered maturity standard optimized for resource-constrained institutions and validated against leakage, detection speed, recovery, and recurrence. Commercial data-quality tools can automate cleaning and matching, but they are products rather than open maturity standards and may assume specialist staffing. R-DAIR addresses the resulting gap by linking open assessment, staged remediation, and operational revenue outcomes.

III. Methodology and R-Dair Framework

A. Research Design and Sample

A multi-stage design combined framework development, expert review, pilot testing, institutional maturity assessment, and operational validation. The analytical architecture comprised 30 institutions, 240 main survey respondents, 12 experts, 40 pilot respondents, and 360 institution-month operational records. Community banks or local deposit-taking institutions represented 46.7% of the sample, credit unions or member-owned institutions 33.3%, and microfinance or community-development financial

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

institutions 20.0%. The instrument contained approximately 40 items across ten validated subdimensions.

Table I. Study Sample and Analytical Units

Unit	n	Purpose
Institutions	30	Maturity/operational validation
Main respondents	240	Institutional assessment
Expert panel	12	Content validity
Pilot respondents	40	Reliability/item refinement
Institution-month records	360	12 months × 30 institutions

B. Four-Domain Architecture

To align the empirical model with the public R-DAIR standard, the ten validated subdimensions were nested under four higher-order domains. Data Quality & Record Integrity captures ownership, integrity controls, reconciliation, and auditability. Anomaly Detection & Revenue Assurance captures continuous monitoring, leakage quantification, and recovery. Workflow & Systems Integration captures exception investigation and escalation/corrective action. Workforce Capability captures operational ownership and root-cause learning, with the workforce dimension operationalized through evidence of accountable roles, escalation competence, corrective-action discipline, and preventive learning. This mapping preserves all validated constructs while presenting a simpler public architecture.

Table Ii. R-Dair Public Domains and Validated Subdimensions

Public domain	Validated subdimensions
Data Quality & Record Integrity	Governance/ownership; data quality controls; reconciliation; auditability
Anomaly Detection & Revenue Assurance	Continuous monitoring; leakage identification; recovery/adjustment
Workflow & Systems Integration	Exception investigation; escalation/corrective action
Workforce Capability	Accountability, control execution, root-cause learning and preventive capability

C. Maturity Scale and Scoring

Each subdimension was scored from Level 1 Reactive (1.00–1.80), Level 2 Controlled (1.81–2.60), Level 3 Standardized (2.61–3.40), Level 4 Continuous (3.41–4.20), to Level 5 Adaptive (4.21–5.00). The institutional score is a weighted composite

$$\mathbf{RDAIR_i = \Sigma_{j=1}^{10} w_j D_{ij}, \quad \Sigma_{j=1}^{10} w_j = 1.}$$

Here, D_{ij} is institution i's score on subdimension j and w_j is the corresponding weight. Because the reported study results did not specify differentiated weights, equal contribution was used for

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

interpretation. The public toolkit can preserve the same baseline while allowing future evidence-based weighting where validated. The five stages provide a prescriptive improvement path: Reactive institutions discover issues after the event; Controlled institutions document periodic checks; Standardized institutions establish repeatable ownership and workflows; Continuous institutions automate stable controls and measure latency; Adaptive institutions use risk-sensitive learning to prevent recurrence.

D. Validation and Statistical Analysis

Twelve experts assessed relevance and clarity using item-level content-validity indices. Pilot testing involved 40 respondents. Internal consistency was evaluated using Cronbach alpha [21]; composite reliability and average variance extracted followed the convergent-validity logic of Fornell and Larcker [22]. Factor structure was assessed using KMO, Bartlett's test, total variance explained, CFI, TLI, RMSEA, and SRMR, interpreted with established fit guidance [23]. Content-validity decisions followed explicit expert-agreement principles [24-26]. Operational validation used reconciliation completeness, leakage rate, mean detection time, unresolved exception rate, recovery rate, recurrence rate, and automation coverage. Pearson correlations tested associations with maturity, while ordinary least-squares regressions estimated outcome change per one-point maturity increase.

E. Open Assessment Toolkit and Practitioner Curriculum

The proposed public implementation converts the maturity instrument into a self-administered assessment workflow rather than a consulting engagement. An institution identifies its revenue-bearing processes, maps critical records and owners, answers evidence-based maturity items, imports or records selected operational indicators, and receives both an overall level and domain-specific remediation priorities. The design deliberately separates maturity evidence from technology choice. A small organization can demonstrate a Controlled or Standardized capability through documented ownership, repeatable reconciliations, exception registers, and closure evidence even when its controls are executed with simple scripts or standard office tools. Conversely, sophisticated anomaly software does not qualify as Continuous or Adaptive if alerts are not traceable, investigated, recovered, and prevented from recurring.

Continuous integrity scoring can be implemented incrementally. At lower levels, the toolkit can calculate scheduled completeness, duplicate, and reconciliation indicators. At Level 4, the same control definitions can run more frequently and report detection and resolution latency. At Level 5, historical exceptions can inform risk-sensitive thresholds and prioritization. This progression reflects the methodological logic in [11] and [12], where structured monitoring is progressively combined with modelling under data constraints, while the weighted decision logic in [17] provides a useful precedent for transparent prioritization across several risk dimensions. The important design requirement is that every automated score remains explainable in terms of source records, control rules, and assigned ownership.

A six-module practitioner curriculum is therefore recommended as part of the standard: revenue-data mapping; data-quality and record-integrity controls; reconciliation and anomaly detection; exception investigation and escalation; recovery and corrective action; and root-cause prevention with maturity reassessment. A capstone should require participants to apply the full assessment to their own data and document before-and-after outcomes. Training is not an ancillary feature because Workforce Capability is one of the four public domains. The curriculum operationalizes that domain by ensuring that staff can interpret alerts, preserve evidence, execute escalation, distinguish true anomalies from noise, and convert lessons learned into preventive control changes.

IV. Results and Discussion

A. Measurement Validation

Expert agreement was strong: average relevance I-CVI was 0.94 and average clarity I-CVI was 0.92. All ten subdimensions were retained, with wording refinement for leakage quantification, escalation evidence, and recovery definition. Reliability and convergent validity were also strong. Cronbach alpha ranged from 0.84 to 0.91, composite reliability from 0.87 to 0.93, and AVE from 0.55 to 0.68. KMO was 0.88, Bartlett's test was significant ($p<0.001$), and the model explained 68.4% of total variance. Global fit was good: CFI=0.955, TLI=0.947, RMSEA=0.049, and SRMR=0.043. These

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

results support the ten subdimensions as related but empirically distinguishable components of the broader four-domain standard.

Table III. Reliability and Convergent Validity

Construct	Mean	α	CR	AVE
Governance/ownership	3.25	.88	.90	.61
Data quality/integrity	3.10	.90	.92	.65
Reconciliation	3.34	.89	.91	.63
Continuous monitoring	2.84	.91	.93	.68
Leakage identification	2.96	.87	.89	.58
Exception investigation	2.91	.86	.88	.57
Escalation/action	3.08	.88	.90	.60
Recovery/adjustment	2.89	.84	.87	.55
Root-cause prevention	2.73	.90	.92	.64
Auditability/oversight	3.22	.89	.91	.62

B. Maturity Distribution

The overall mean R-DAIR score was 2.99, placing the typical institution at the Standardized level. Four institutions (13.3%) were Reactive, seven (23.3%) Controlled, nine (30.0%) Standardized, seven (23.3%) Continuous, and three (10.0%) Adaptive. Reconciliation had the highest mean (3.34), followed by governance and ownership (3.25) and auditability/oversight (3.22). Root-cause prevention was lowest (2.73), followed by continuous monitoring (2.84), recovery (2.89), and exception investigation (2.91). The ordering is consistent with staged maturity theory [15], [16]: formalized controls and ownership tend to precede closed-loop monitoring, recovery, and adaptive prevention.

Table IV. Institutional Maturity Distribution

Level	n	%	Mean
Reactive	4	13.3	1.52
Controlled	7	23.3	2.30
Standardized	9	30.0	3.04
Continuous	7	23.3	3.79
Adaptive	3	10.0	4.54

C. Operational Performance Across Maturity Levels

Operational performance improved monotonically with maturity. Reconciliation completeness increased from 84.0% at Reactive to 98.0% at Adaptive. Revenue leakage declined from 1.75% to 0.38%, mean detection time from 11.5 to 2.7 days, unresolved exceptions from 16.0% to 4.0%, and recurrence from 17.4% to 5.0%. Recovery increased from 45.0% to 84.2%, while automation coverage increased from 30.0% to 84.6%. Relative to Reactive institutions, Adaptive institutions therefore exhibited about 78.3% lower leakage, 76.5% shorter detection time, 75.0% fewer unresolved exceptions, and 71.3% lower recurrence. The result supports the proposition that continuous revenue assurance is a connected system of governance, detection, response, recovery, and learning rather than merely a software deployment.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

The decline in detection latency is particularly important for the open-standard endeavor. A self-administered toolkit that measures latency can give institutions a directly interpretable performance indicator rather than an opinion-based maturity score. The same applies to recovery and recurrence: the standard can test whether detected exceptions produce recovered value and whether root causes are actually eliminated. This outcome-linked structure differentiates R-DAIR from maturity assessments that classify practices without demonstrating operational consequence.

D. Correlation and Regression Results

The strongest bivariate association was between maturity and mean detection time ($r=-0.814$, $p<0.001$). A one-point increase in R-DAIR corresponded to a 3.104-day reduction in detection time ($R^2=0.663$). This finding is consistent with continuous-auditing theory [5], [6] and with the emphasis on timely anomaly detection in high-speed payment environments [7]. Revenue leakage was also strongly lower at higher maturity ($r=-0.743$, $p<0.001$); the regression slope was -0.448 percentage points per maturity point ($R^2=0.552$). Thus, the maturity construct is directly associated with the financial outcome it is intended to improve.

Reconciliation completeness increased with maturity ($r=0.750$, $p<0.001$; slope=+4.322 percentage points; $R^2=0.563$), and unresolved exceptions decreased ($r=-0.740$; slope=-3.794 percentage points; $R^2=0.547$). Recovery showed a strong positive association ($r=0.788$; slope=+12.816 percentage points; $R^2=0.621$), while recurrence declined ($r=-0.745$; slope=-4.167 percentage points; $R^2=0.556$). Control automation correlated positively with maturity ($r=0.804$, $p<0.001$). Automation should not be interpreted as sufficient by itself, however; governance and quality-assurance scholarship [8]-[10] supports the need for accountable ownership, evidence, and escalation, while [13] cautions against substituting unverified AI output for auditable control evidence.

Table V. Correlation and Regression Summary

Outcome	r	Slope / +1 maturity	R^2
Reconciliation	+.750	+4.322 pp	.563
Revenue leakage	-.743	-0.448 pp	.552
Detection time	-.814	-3.104 days	.663
Unresolved exceptions	-.740	-3.794 pp	.547
Revenue recovery	+.788	+12.816 pp	.621
Leakage recurrence	-.745	-4.167 pp	.556
Automation coverage	+.804	Not reported	—

E. Implications for the Open R-DAIR Endeavor

All seven directional hypotheses were supported. The findings provide an empirical basis for the proposed open standard because they demonstrate that the maturity score is not merely descriptive. Higher levels correspond with more complete reconciliation, lower leakage, faster detection, fewer unresolved exceptions, stronger recovery, lower recurrence, and broader automation. The four-domain public structure can therefore be paired with evidence-based remediation maps. For example, a low Data Quality & Record Integrity score accompanied by low reconciliation completeness points toward source-to-ledger mapping and record ownership; a low Anomaly Detection & Revenue Assurance score with long detection latency supports investment in automated matching or threshold monitoring; and a low Workforce Capability score combined with high recurrence indicates that technical detection is not being converted into root-cause learning.

ISSN:2584-2706 DOI: https://doi.org/10.5281/zenodo.22161707

The framework also accommodates resource constraints. The studies by Adeyekun et al. [11] and Adeyekun [12] are useful not because their environmental application is financially equivalent, but because they demonstrate the broader methodological value of structured data-driven monitoring and predictive assessment in data-limited contexts. Similarly, the composite governance approach in [17] supports prioritizing finite resources according to measured risk rather than technology sophistication. R-DAIR therefore offers a staged pathway in which smaller institutions can progress from documented controls to continuous monitoring and finally to risk-sensitive adaptive prevention without assuming enterprise-scale infrastructure at the outset.

F. Pilot Measures and Success Criteria

For dissemination and field validation, success should be measured with operational indicators that can be reproduced by institutions themselves. Recommended pilot measures include duplicate-record rate, completeness of critical revenue fields, reconciliation completeness, mean detection latency, exception aging, recovery rate, recurrence rate, and the proportion of defined controls executed automatically or continuously. These measures correspond directly to the study outcomes and allow a pilot to show whether an intervention changes the control environment rather than merely improving user perceptions. A before-and-after design can also identify which maturity-domain improvements produce the largest operational gains and can supply anonymized calibration profiles for later versions of the standard.

The empirical slopes provide useful, but not prescriptive, reference points for those pilots. The observed association of a one-point maturity increase with a 3.104-day reduction in detection time and a 0.448-percentage-point reduction in leakage indicates the scale of improvement that may be operationally meaningful, but these values should not be converted into universal benchmarks until replicated across sectors and jurisdictions. Pilot reporting should therefore emphasize direction, magnitude, reproducibility, and control evidence. This approach keeps the standard evidence-based while avoiding the false precision that could arise from treating one validation sample as a universal performance norm.

V. Conclusion and Recommendations

A. Conclusion

This study developed and validated R-DAIR as the empirical foundation of the Open Revenue Data Assurance, Integrity & Reliability Standard. The public standard contains four domains and five maturity levels, while the underlying instrument retains ten validated subdimensions for diagnostic precision. Content validity, internal consistency, convergent validity, and global fit were strong, and the typical participating institution was Standardized rather than Continuous. Most importantly, higher maturity was associated with materially better operational outcomes. These relationships give the framework criterion relevance and support its use as more than a descriptive checklist.

The evidence also supports the proposed endeavor's technology-neutral positioning. Continuous assurance can be improved through defined ownership, standardized reconciliations, exception routing, measured detection latency, recovery discipline, and root-cause correction before predictive analytics are introduced. Where AI is used, it should remain subordinate to validated data, traceable controls, and accountable review. This makes the framework suitable for an open, vendor-neutral, self-administered standard rather than a proprietary software model.

B. Implementation and Dissemination Recommendations

Reactive and Controlled organizations should first inventory revenue streams, define critical data elements, name record owners, document system-to-ledger mappings, standardize leakage definitions, and establish formal exception responsibility. Standardized institutions should automate stable high-volume reconciliations, centralize exception queues, measure detection and resolution latency, and establish risk-based escalation thresholds. Continuous institutions should connect monitoring to recovery, root-cause analysis, control redesign, and recurring control-health indicators. Adaptive institutions should use risk-sensitive analytics and feedback loops to refine thresholds and prevent repeated failure.

For the proposed open endeavor, the assessment toolkit should report both maturity scores and outcome measures so users can see whether process improvements produce measurable effects.

Recommended pilot indicators include duplicate-rate reduction, reconciliation completeness, detection-latency reduction, unresolved-exception aging, recovery rate, and recurrence. A practitioner curriculum should teach record ownership, control design, exception management, interpretation of maturity profiles, and evidence-based remediation. Distribution through trusted SME, credit-union, cooperative, and community-banking networks can preserve zero or low barriers to adoption while generating anonymized calibration profiles for future validation.

C. Limitations and Future Work

The institutional sample of 30 limits broad generalization, and the available results do not report jurisdiction, asset size, technology architecture, or regulatory regime. The cross-sectional design supports association rather than causation. Future work should validate R-DAIR longitudinally, evaluate alternative weighting schemes, expand formal testing to nonfinancial SMEs and cooperatives, and use verified de-identified field-level data for multilevel analysis across the 360 institution-month observations. The supplied institution-level analytical table was explicitly labelled synthetic; therefore, publication-quality replication should replace it with verified raw or de-identified observations where available. Future research should also evaluate inter-rater reliability of self-administration, calibration stability across sectors, and whether movement between maturity levels predicts subsequent reductions in leakage and detection latency.

References

[1] R. Y. Wang and D. M. Strong, “Beyond accuracy: What data quality means to data consumers,” Journal of Management Information Systems, vol. 12, no. 4, pp. 5–33, 1996, doi: 10.1080/07421222.1996.11518099.
[2] Y. W. Lee, D. M. Strong, B. K. Kahn, and R. Y. Wang, “AIMQ: A methodology for information quality assessment,” Information & Management, vol. 40, no. 2, pp. 133–146, 2002, doi: 10.1016/S0378-7206(02)00043-5.
[3] L. L. Pipino, Y. W. Lee, and R. Y. Wang, “Data quality assessment,” Communications of the ACM, vol. 45, no. 4, pp. 211–218, 2002, doi: 10.1145/505248.506010.
[4] Basel Committee on Banking Supervision, Principles for Effective Risk Data Aggregation and Risk Reporting. Basel, Switzerland: Bank for International Settlements, 2013.
[5] M. G. Alles, F. Tostes, M. A. Vasarhelyi, and E. L. Riccio, “Continuous auditing: The USA experience and considerations for its implementation in Brazil,” Journal of Information Systems and Technology Management, vol. 3, no. 2, pp. 211–224, 2006, doi: 10.4301/S1807-17752006000200008.
[6] M. G. Alles, A. Kogan, and M. A. Vasarhelyi, “Putting continuous auditing theory into practice: Lessons from two pilot implementations,” Journal of Information Systems, vol. 22, no. 2, pp. 195–214, 2008, doi: 10.2308/jis.2008.22.2.195.
[7] A. J. Olaseinde, “The speed of theft: Developing real-time detection protocols for authorized push payment (APP) fraud in instant payment systems,” Journal of Computational Analysis and Applications, vol. 33, no. 6, 2024.
[8] V. Khatri and C. V. Brown, “Designing data governance,” Communications of the ACM, vol. 53, no. 1, pp. 148–152, 2010, doi: 10.1145/1629175.1629210.
[9] Committee of Sponsoring Organizations of the Treadway Commission, Internal Control—Integrated Framework. Durham, NC, USA: COSO, 2013.
[10] M. B. Ashimolowo and A. G. Oginni, “Quality governance and performance stability in high-risk projects: A framework for strategic assurance,” International Journal of Scientific Research and Modern Technology, vol. 1, no. 2, pp. 16–40, 2022, doi: 10.38124/ijsrmt.v1i2.1282.
[11] A. A. Adeyekun, O. H. Orekoya, and O. A. Abiola, “Data-driven monitoring and modelling of coastal and sedimentary systems for climate resilience,” International Journal of Data Science and Engineering, vol. 1, no. 1, pp. 10–42, 2023, doi: 10.34218/IJDSE_01_01_002.
[12] A. A. Adeyekun, “Artificial intelligence framework for predictive sediment dynamics and environmental vulnerability assessment in data-limited coastal systems,” Journal of Computational Analysis and Applications, vol. 33, no. 2, 2024.
[13] A. J. Olaseinde and B. B. Azeez, “The trust paradox: Analyzing auditor reliance on hallucinating generative AI models in internal control testing,” International Journal of Artificial Intelligence

Engineering and Transformation, vol. 3, no. 1, pp. 38–49, 2022, doi: 10.54660/IJAIET.2022.3.1.38-49.
[14] T. de Bruin, R. Freeze, U. Kulkarni, and M. Rosemann, "Understanding the main phases of developing a maturity assessment model," in Proc. 16th Australasian Conf. Information Systems (ACIS), 2005.
[15] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing maturity models for IT management—A procedure model and its application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, 2009, doi: 10.1007/s12599-009-0044-5.
[16] J. Pöppelbuß and M. Röglinger, "What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management," in Proc. 19th European Conf. Information Systems (ECIS), 2011.
[17] M. B. Ashimolowo, "A computational model for risk-based quality governance assessment in high-risk infrastructure projects: A weighted composite scoring approach," Journal of Computational Analysis and Applications, vol. 33, no. 8, 2024.
[18] International Organization for Standardization, ISO 8000-61:2016 Data Quality—Part 61: Data Quality Management—Process Reference Model. Geneva, Switzerland: ISO, 2016.
[19] EDM Council, "Data Management Capability Assessment Model (DCAM)," EDM Council. [Online]. Available: https://edmcouncil.org/frameworks/dcam/. Accessed: 2024.
[20] M. A. Vasarhelyi, A. Kogan, and B. M. Tuttle, "Big data in accounting: An overview," Accounting Horizons, vol. 29, no. 2, pp. 381–396, 2015, doi: 10.2308/acch-51071.
[21] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," Psychometrika, vol. 16, no. 3, pp. 297–334, 1951, doi: 10.1007/BF02310555.
[22] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, vol. 18, no. 1, pp. 39–50, 1981, doi: 10.1177/002224378101800104.
[23] L. Hu and P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," Structural Equation Modeling, vol. 6, no. 1, pp. 1–55, 1999, doi: 10.1080/10705519909540118.
[24] D. F. Polit and C. T. Beck, "The content validity index: Are you sure you know what is being reported? Critique and recommendations," Research in Nursing & Health, vol. 29, no. 5, pp. 489–497, 2006, doi: 10.1002/nur.20147.
[25] Abagna, E. (2024). FraudLens AI for intelligent claims forensics and real-time insurance fraud detection in the United States. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(4), 1161–1176. https://doi.org/10.32628/CSEIT261233040
[26] Fowowe, O. (2025). An integrated AI-driven agricultural financial intelligence framework for farm revenue forecasting, tax compliance efficiency, and subsidy allocation in the United States. International Journal of Scientific Research in Artificial Intelligence and Machine Learning, 1(3), 52–62.