American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Continuous Auditing Readiness in Cloud-Based Small Enterprises

Joshua Onome Imoniana

Professor, University of São Paulo (USP), Brazil

Abstract

Cloud computing has enabled small enterprises to adopt accounting, payment, inventory, payroll, customer-management, and operational systems without maintaining extensive local information-technology infrastructure. Although this transition can improve accessibility and integration, it also changes the environment in which audit evidence is generated, retained, secured, and reviewed. Continuous auditing offers a potential response by enabling audit-related procedures and control evaluations to occur more frequently than conventional periodic examinations. However, the technical availability of cloud data does not automatically make an enterprise ready for continuous auditing. Readiness depends on structured audit trails, stable data interfaces, access-control discipline, automated control evidence, data quality, cybersecurity governance, exception-management procedures, and management capability.

The present study develops a simulation-based framework for examining continuous auditing readiness in cloud-based small enterprises. A synthetic analytical sample of 480 observations is distributed across four hypothetical maturity conditions: fragmented cloud controls, basic digitized controls, integrated cloud controls, and continuous-monitoring-enabled controls. Continuous auditing readiness represents the principal outcome, while data integration, audit-trail completeness, control automation, and cybersecurity and access readiness are examined as associated dimensions. Simulated mean readiness increases from 2.47 in the fragmented-control condition to 4.32 under continuous-monitoring-enabled controls.

A separate continuous simulation of 180 observations produces a positive association between cloud control maturity and continuous auditing readiness, $r = .800$. The study argues that cloud adoption should be distinguished from audit readiness: continuous auditing becomes feasible only when digital records are reliable, accessible, controlled, and capable of supporting repeatable automated tests.

Keywords: continuous auditing; cloud accounting; small enterprises; audit readiness; internal controls; data analytics; cloud computing; continuous monitoring

1. Introduction

Small enterprises increasingly rely on cloud-based applications for financial accounting, invoicing, payroll, procurement, inventory management, electronic payments, customer relationship management, document storage, and other business processes. Cloud computing offers a model in which configurable computing resources can be accessed on demand without requiring every organization to own and

administer extensive physical infrastructure. Mell and Grance's widely adopted cloud-computing framework emphasized characteristics such as on-demand access, resource pooling, broad network availability, rapid elasticity, and measured service. For small enterprises, these characteristics can reduce infrastructure barriers and allow sophisticated business applications to be used through subscription-oriented arrangements. Yet migration from locally maintained systems to distributed cloud services changes the technological and control environment in which accounting information is generated and preserved.

Auditing has traditionally been organized around periodic examination. Auditors select transactions, evaluate controls, obtain supporting documentation, perform substantive procedures, and form conclusions about information covering a defined reporting period. Rezaee and colleagues argued that advances in digital systems create possibilities for continuous auditing, while Alles, Kogan, and Vasarhelyi examined the economic and technological feasibility of more continuous assurance processes. Continuous auditing does not necessarily imply an uninterrupted external audit of every transaction. It is better understood as the use of automated or frequently executed audit procedures to evaluate transactions, controls, anomalies, or risk indicators at shorter intervals than conventional retrospective auditing. The availability of cloud-based transactional data can make such procedures technically more accessible, but data availability alone is insufficient.

A small enterprise may use several cloud platforms simultaneously, each with different authentication mechanisms, data structures, logging practices, retention rules, and application programming interfaces. Accounting may reside in one application, inventory in another, payments with multiple providers, payroll on a separate platform, and supporting documents in a cloud-storage environment. Such fragmentation can create substantial challenges for audit automation. A transaction recorded in the general ledger may need to be reconciled with a payment record, purchase authorization, inventory movement, tax record, and digital invoice stored elsewhere. Continuous auditing therefore requires more than digital transactions; it requires sufficiently stable relationships among data sources to permit repeatable extraction, validation, reconciliation, and exception analysis.

Control maturity is similarly critical. Cloud applications can produce detailed activity logs and automated workflow records, but these records provide meaningful audit evidence only when identities are properly managed, user privileges are controlled, timestamps are reliable, configurations are documented, and records cannot be altered without traceability. The Committee of Sponsoring Organizations of the Treadway Commission's internal-control framework emphasizes the interdependence of control environment, risk assessment, control activities, information and communication, and monitoring. In cloud-based small enterprises, these elements remain relevant even where technology providers perform significant portions of infrastructure management. Management cannot transfer accountability for financial reporting, authorization, access control, or data governance simply by outsourcing the underlying application platform.

The present study therefore examines continuous auditing readiness in cloud-based small enterprises as a multidimensional organizational capability rather than a binary technological condition. Because no primary dataset from actual small enterprises has been supplied, the manuscript is explicitly structured as a simulation-based research article. Synthetic observations are used to illustrate how differences in cloud-control maturity might be associated with audit readiness without fabricating

empirical findings. The proposed framework integrates data integration, audit-trail completeness, control automation, cybersecurity and access readiness, and organizational governance. Its central proposition is that cloud adoption creates the technical foundation for more frequent assurance, but continuous auditing becomes viable only when digital processes are sufficiently standardized, traceable, controlled, and analytically accessible.

2. Objectives of the Study

2.1 To Assess Continuous Auditing Readiness Across Cloud-Control Maturity Levels

The primary objective is to examine how continuous auditing readiness may differ among small enterprises operating at different levels of cloud-control maturity. The study distinguishes fragmented cloud environments from basic digitized environments, integrated cloud-control environments, and systems incorporating continuous-monitoring capabilities. This progression recognizes that using cloud accounting software is not equivalent to possessing an audit-ready digital architecture. Two enterprises may use similar accounting applications yet differ substantially in logging, interface integration, segregation of duties, data retention, user-access governance, and exception management.

Continuous auditing readiness is therefore conceptualized as the capacity of the enterprise's information and control environment to support frequent, repeatable, and reliable audit procedures. Such procedures may include automated reconciliations, duplicate-payment detection, unusual journal-entry analysis, access-right reviews, exception testing, transaction-sequence analysis, master-data monitoring, and other forms of digitally enabled assurance. The objective is not to prescribe a universal technical architecture but to identify the underlying conditions that make these procedures credible.

2.2 To Examine Data Integration, Audit Trails, and Control Automation

A second objective is to assess the contribution of data integration, audit-trail completeness, and automated controls to continuous auditing readiness. Continuous testing requires data to be obtainable in a structured form and connected across relevant processes. Where evidence remains distributed among unrelated applications, spreadsheets, emails, and manually retained documents, automation becomes more difficult and audit procedures remain dependent on repeated human reconstruction of transaction histories.

Audit-trail completeness is equally important because continuous auditing depends on the ability to reconstruct who initiated, approved, modified, and completed a transaction. Automated controls can strengthen this environment when systems enforce approval thresholds, segregation rules, required fields, exception flags, or reconciliation procedures consistently. However, automation is valuable only when configurations are authorized and periodically reviewed. Poorly configured automated controls can create a false impression of reliability because incorrect logic may be applied consistently at scale.

2.3 To Evaluate Cybersecurity and Governance as Audit-Readiness Conditions

The third objective is to examine cybersecurity and access governance as foundational components of continuous auditing readiness. Cloud-based systems expand reliance on digital identities, remote connectivity, third-party providers, and interconnected applications. An audit process cannot place

strong reliance on digital evidence if users share credentials, privileged access is not reviewed, multifactor authentication is inconsistently applied, or activity logs are incomplete.

The objective therefore positions cybersecurity not as a separate technical concern but as part of evidence reliability. Continuous auditing readiness requires management to understand where critical records reside, who can access them, how changes are logged, what happens when employees leave, how service-provider responsibilities are defined, and how incidents affecting data integrity are identified and escalated.

3. Review of Literature

3.1 Evolution of Continuous Auditing and Automated Assurance

Rezaee, Sharbatoghlie, Elam, and McMickle described continuous auditing as an approach made increasingly feasible by advances in electronic processing and digital evidence. Their work emphasized that contemporary accounting systems create opportunities for automated procedures that can reduce the delay between economic events and audit evaluation. Alles, Kogan, and Vasarhelyi similarly examined the feasibility and economics of continuous assurance, arguing that technological integration changes both the cost structure and timing of audit procedures.

Vasarhelyi, Alles, and Kogan advanced the concept further by discussing analytic monitoring principles for continuous assurance. Rather than treating auditing solely as repeated transaction checking, their work highlighted the role of models, expectations, and exception identification. Continuous auditing can therefore be understood as a shift from periodic evidence collection toward ongoing identification of deviations that deserve human attention. This approach is particularly relevant to small enterprises because limited audit resources can potentially be directed toward unusual or high-risk transactions rather than repeatedly inspecting routine transactions that satisfy established control parameters.

Alles and colleagues' pilot work involving continuous monitoring of business-process controls demonstrated the practical importance of integrating automated testing with actual organizational processes. Their research also exposed a persistent implementation challenge: the existence of technically available data does not guarantee that organizations have governance structures, process standardization, or management incentives necessary to use continuous monitoring effectively. The same issue remains relevant to cloud-based small enterprises, where applications may be technically sophisticated but local control processes may be informal.

Later research expanded the discussion toward analytics and increasingly automated audit environments. Earley examined the opportunities and challenges associated with audit data analytics, while Cao, Chychyla, and Stewart considered the potential contribution of big-data analytics to financial-statement auditing. Appelbaum, Kogan, and Vasarhelyi subsequently argued that contemporary audit engagements require broader research on how large and diverse datasets can be incorporated into assurance. These developments reinforce a central theme: auditing becomes more continuous and analytical only when underlying information is sufficiently reliable and accessible.

3.2 Cloud Computing, Small Enterprises, and Information Integration

Cloud computing changed the economics of information systems by enabling enterprises to access infrastructure, platforms, and software through remote services. Armbrust and colleagues described cloud computing as a major transformation in the provisioning and economics of computing resources. Marston and colleagues examined its business implications, emphasizing scalability, flexibility, and potential changes to organizational technology investment.

Small and medium-sized enterprises have attracted particular attention because cloud services can reduce the capital and specialist expertise required for information-system adoption. Gupta, Seetharaman, and Raj examined adoption of cloud computing among small and medium businesses and identified the importance of factors such as cost reduction, ease of use, convenience, and reliability. Alshamaila, Papagiannidis, and Li similarly developed a multi-perspective framework for cloud adoption among SMEs, showing that technological, organizational, and environmental considerations interact in adoption decisions. Low, Chen, and Wu also demonstrated that organizational and technological characteristics influence cloud adoption.

These studies largely explain why smaller enterprises adopt cloud services, but adoption and continuous-audit readiness represent different analytical questions. Cloud systems may improve data availability while simultaneously increasing reliance on third-party providers. An enterprise may gain automated transaction processing yet lose direct control over infrastructure management. It may have detailed system logs but lack internal knowledge concerning how those logs should be interpreted. Readiness therefore requires understanding the allocation of responsibilities between the enterprise and service provider.

Oliveira, Thomas, and Espadanal demonstrated that cloud adoption varies according to organizational context and technology characteristics. For continuous auditing, this implies that readiness assessment should consider the practical configuration of each enterprise rather than assuming that all organizations using cloud services possess equivalent technical maturity. Small enterprises can be particularly heterogeneous because some operate almost entirely through standardized software-as-a-service platforms while others combine new cloud applications with legacy systems, spreadsheets, manual approvals, and informal recordkeeping.

3.3 Internal Control, Data Analytics, and Cloud Assurance Risks

Internal controls remain central to the reliability of cloud-generated audit evidence. The COSO framework establishes that monitoring and information systems must operate within a broader internal-control structure. Cloud deployment changes how controls are implemented but does not eliminate the need for authorization, segregation of duties, reconciliation, supervision, documentation, and risk assessment. Some controls may migrate from manual procedures to automated workflows, while others become shared responsibilities between the enterprise and technology provider.

Alles, Gray, Cao, Chychyla, Stewart, and related audit-analytics scholars have emphasized that access to larger digital datasets can improve audit coverage but also creates challenges concerning data provenance, completeness, standardization, and interpretation. An automated test can produce precise output while still being unreliable if the extracted dataset excludes transactions, contains inconsistent identifiers, or does not capture modifications made outside the principal system.

Cybersecurity further affects audit evidence. Cloud environments depend heavily on digital identity management, access permissions, and logging. The National Institute of Standards and Technology's security-control frameworks and the Cloud Security Alliance's guidance emphasize controls around access, configuration, monitoring, incident response, and data protection. In continuous auditing, these areas directly influence whether evidence can be trusted. A transaction log has limited assurance value when unauthorized users can alter underlying records or when privileged actions are insufficiently monitored.

The literature therefore indicates a research gap between the availability of cloud technology and the organizational capability to support continuous auditing within small enterprises. Much prior research has examined either continuous auditing in larger integrated environments or cloud adoption from the perspective of technology use. The present study connects these streams by conceptualizing continuous auditing readiness as a multidimensional state involving integrated data, reliable audit trails, automated controls, security governance, and repeatable analytical access.

4. Research Methodology

4.1 Research Design and Simulation Framework

The study employs a simulation-based comparative design. It does not claim to report data collected from actual enterprises, auditors, accountants, or cloud-service providers. Synthetic observations were generated to demonstrate how continuous auditing readiness could be studied while maintaining a clear distinction between methodological illustration and empirical evidence.

The simulation contains 480 observations distributed equally across four hypothetical cloud-control maturity conditions. The fragmented-control condition represents enterprises where multiple cloud applications operate with limited integration and substantial manual intervention. The basic digitized condition represents enterprises that use cloud accounting and supporting applications but retain relatively simple controls. The integrated condition represents enterprises with standardized data flows, stronger access management, and more complete audit trails. The continuous-monitoring-enabled condition represents environments where automated controls and exception-monitoring procedures are embedded more systematically.

Table 1: Proposed Simulation Design and Continuous Auditing Readiness Framework

Research Component	Operational Specification
Research design	Simulation-based comparative study
Synthetic analytical sample	480 observations
Observations per maturity condition	120
Condition 1	Fragmented cloud controls

Research Component	Operational Specification
Condition 2	Basic digitized controls
Condition 3	Integrated cloud controls
Condition 4	Continuous-monitoring-enabled controls
Primary outcome	Continuous auditing readiness
Readiness dimensions	Data integration, audit-trail completeness, control automation, cybersecurity and access readiness
Illustrative measurement	Five-point maturity scales
Supporting analysis	One-way ANOVA and correlation analysis
Additional continuous simulation	180 synthetic observations
Data status	Entirely synthetic
Human or enterprise participants	None

Note: The values reported in this paper are generated exclusively for methodological demonstration. They must not be described as observations obtained from real small enterprises.

4.2 Operationalization of Continuous Auditing Readiness

Continuous auditing readiness is defined as the organizational and technological capacity to execute repeatable, sufficiently reliable, and relatively frequent automated or semi-automated audit procedures. A future empirical instrument could assess whether the enterprise can retrieve transaction populations without manual reconstruction, reconcile identifiers across applications, retain complete change histories, detect control exceptions, review privileged access, and provide reliable timestamps and digital evidence.

Data integration refers to the degree to which relevant financial and operational information can be consistently connected across cloud applications. Audit-trail completeness measures whether transaction creation, modification, authorization, and completion are traceable. Control automation captures the extent to which routine preventive or detective controls are system enforced rather than dependent exclusively on informal manual procedures.

Cybersecurity and access readiness measures whether the enterprise maintains appropriate identity, privilege, authentication, logging, termination, and incident-management practices. In a future

empirical investigation, these dimensions should be assessed separately because an enterprise can possess technically integrated applications while remaining weak in access governance. A composite readiness score should therefore be constructed only after reliability and dimensional validity are evaluated.

4.3 Analytical Procedure and Research Integrity

The four maturity groups were simulated around progressively stronger theoretical readiness levels. Individual variability was introduced within each group so that the data would not imply that all enterprises at the same maturity stage behave identically. Descriptive statistics were used to compare readiness dimensions, and a one-way analysis of variance was employed to illustrate between-condition differentiation.

A separate synthetic dataset of 180 observations was generated to examine the relationship between cloud control maturity and continuous auditing readiness as continuous variables. The resulting Pearson correlation was r = .800, indicating a strong positive relationship within the simulated model. The correlation was not engineered as evidence of an observed population relationship and therefore should not be used for external inference.

Because no actual enterprises, employees, client files, audit records, financial statements, system logs, or identifiable information were analyzed, no institutional ethics approval or organizational consent is claimed. A future empirical study involving enterprise records should implement confidentiality agreements, secure data handling, restricted access to system logs, and appropriate governance procedures because audit-readiness assessments can expose commercially sensitive control weaknesses.

5. Analysis

5.1 Continuous Auditing Readiness Across Maturity Conditions

The simulated analysis demonstrates a progressive increase in continuous auditing readiness across the four cloud-control maturity conditions. Fragmented cloud environments produce the lowest mean readiness score at 2.47. This condition represents enterprises that have adopted cloud applications without establishing strong integration, standardized audit trails, or consistent control automation.

Basic digitized controls raise the simulated readiness mean to 3.06. This indicates that adoption of cloud accounting and related digital tools can create a useful foundation but may remain insufficient for frequent automated auditing when manual reconciliations and disconnected applications continue to dominate critical processes.

Table 2: Simulated Continuous Auditing Readiness Across Cloud-Control Maturity Conditions

Cloud-Control Maturity Condition	Continuous Auditing Readiness	Data Integration	Audit-Trail Completeness	Control Automation	Cybersecurity and Access Readiness
Fragmented cloud	2.47	2.36	2.56	2.22	2.68

Cloud-Control Maturity Condition	Continuous Auditing Readiness	Data Integration	Audit-Trail Completeness	Control Automation	Cybersecurity and Access Readiness
controls					
Basic digitized controls	3.06	3.10	3.21	2.95	3.26
Integrated cloud controls	3.75	3.86	4.01	3.79	3.92
Continuous-monitoring-enabled controls	4.32	4.40	4.42	4.44	4.35

The table illustrates that continuous auditing readiness does not rise through a single dimension. Improvements occur simultaneously across integration, traceability, automated control operation, and access governance. The strongest condition therefore represents a coordinated control environment rather than merely an enterprise possessing more software.

5.2 Relationship Between Cloud Control Maturity and Audit Readiness

The continuous simulation reinforces the group-level pattern. Across 180 synthetic observations, cloud control maturity and continuous auditing readiness show a strong positive correlation of r = .800. The relationship suggests that more mature control environments provide increasingly favorable conditions for continuous assurance techniques.

The result should nevertheless be interpreted carefully. High cloud maturity does not guarantee audit readiness automatically. A technically advanced enterprise can remain difficult to audit continuously if data ownership is unclear, logs are incomplete, system interfaces change frequently, or control responsibilities between management and service providers are poorly documented.

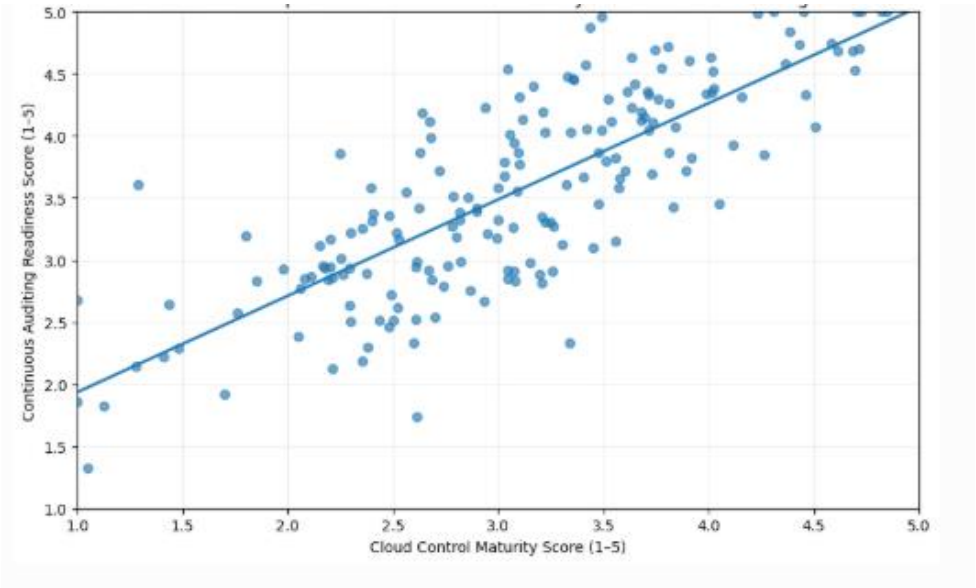
Conversely, a smaller enterprise using relatively simple technology may still achieve meaningful continuous-audit capability if its processes are highly standardized and its data are complete. Readiness therefore depends on the quality of control architecture and evidence, not on organizational size or expenditure on technology alone.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.3 Graphical Interpretation of the Simulated Relationship

Graph 1: Simulated Relationship Between Cloud Control Maturity and Continuous Auditing Readiness



Key Finding: Higher cloud-control maturity is associated with stronger simulated continuous auditing readiness, although considerable enterprise-level variation remains around the overall relationship.

The dispersion in the graph is analytically important. Enterprises with similar overall maturity scores can exhibit different levels of readiness because specific weaknesses may constrain audit automation. For example, strong transaction integration cannot fully compensate for weak privilege management, while complete logs provide limited benefit when transaction identifiers cannot be reconciled across systems.

The graphical relationship therefore supports a multidimensional maturity interpretation. Continuous auditing readiness should be assessed through specific control and data capabilities rather than inferred from the presence of cloud accounting software or the general degree of digitalization.

6. Discussion

6.1 Cloud Adoption Is Not Equivalent to Continuous Auditing Readiness

The principal implication of the simulation is that cloud adoption should be distinguished clearly from audit readiness. Cloud applications can make information more accessible, but they can also distribute evidence across multiple providers and systems. An enterprise may therefore appear digitally advanced while still requiring extensive manual effort before auditors can reconstruct complete transaction populations.

This distinction is especially important for small enterprises because cloud adoption is often driven by operational simplicity rather than audit architecture. Management may select separate applications for accounting, payments, payroll, inventory, and document storage because each solves an immediate business problem. Over time, however, these independent decisions can produce fragmented evidence flows. Continuous auditing requires greater attention to how systems interact and whether transactions can be followed end to end.

The transition toward readiness therefore begins with process mapping and data understanding. Enterprises need to identify critical transaction streams, relevant applications, authoritative data sources, integration points, responsible users, and the evidence retained at each stage. Without this foundation, automated audit procedures risk testing incomplete or misunderstood datasets.

6.2 Audit Trails, Automated Controls, and Exception-Oriented Assurance

A second implication concerns the movement from manual evidence collection toward exception-oriented assurance. Continuous auditing becomes most valuable when routine transactions can be tested automatically against defined expectations and human attention can be directed toward anomalies. Duplicate payments, unusual journal entries, unauthorized master-data changes, transactions outside normal working patterns, excessive credit overrides, or segregation-of-duty conflicts are examples of conditions that may be monitored more frequently.

This approach depends heavily on complete audit trails. Automated exception detection is credible only when the data capture all relevant events. If manual adjustments occur outside the system or logs fail to record privileged changes, automated procedures can provide false reassurance. Audit-trail quality should therefore be evaluated before sophisticated analytical models are introduced.

Control automation similarly requires governance. A workflow that automatically prevents purchases beyond an authorized threshold may strengthen control consistency, but the control is useful only when thresholds are correct and access to change the configuration is restricted. Continuous auditing should therefore examine both operational transactions and the configuration settings that determine how automated controls behave.

6.3 Practical Implications for Small Enterprises and Auditors

Small enterprises do not need to reproduce the technology environments of large corporations to become more audit ready. A practical progression can begin with standardized chart-of-account structures, unique transaction identifiers, disciplined user-access management, consistent digital document retention, automated bank reconciliation, documented approval workflows, and periodic review of system logs.

Cloud-service providers can support readiness when they make structured exports, reliable application programming interfaces, access logs, role definitions, change histories, and service-control information readily available. However, management remains responsible for understanding which controls are performed by the provider and which remain the responsibility of the enterprise. This shared-responsibility distinction should be documented rather than assumed.

Auditors also need to adapt their procedures. Continuous auditing readiness should not simply lead to more frequent execution of traditional tests. It creates an opportunity to redesign audit procedures around full-population analysis, automated control evaluation, exception thresholds, and trend monitoring. Human professional judgment remains necessary for determining materiality, interpreting anomalies, evaluating business context, and assessing whether automated evidence is sufficiently reliable.

7. Conclusion

Cloud-based business systems create favorable conditions for more frequent and data-driven assurance, particularly for small enterprises that previously lacked access to integrated information infrastructure. However, the use of cloud accounting or other software-as-a-service applications does not in itself establish continuous auditing readiness. Readiness depends on whether financial and operational data can be reliably retrieved, connected, traced, protected, and tested through repeatable procedures.

The simulation presented in this study demonstrates a progressive increase in continuous auditing readiness from fragmented cloud controls to continuous-monitoring-enabled environments. Mean simulated readiness rises from 2.47 under fragmented controls to 3.06 under basic digitized controls, 3.75 under integrated controls, and 4.32 in the continuous-monitoring-enabled condition. A separate continuous simulation produces a strong positive association between cloud control maturity and continuous auditing readiness, $r = .800$. These values are synthetic and must not be presented as findings from actual enterprises.

The analysis suggests that the most important transition is not simply from manual accounting to cloud accounting, but from isolated digital applications to a controlled information ecosystem. Data integration, complete audit trails, automated controls, access governance, security monitoring, and clear allocation of responsibilities collectively determine whether digital evidence can support continuous assurance. Weakness in any of these areas can constrain automation even when the underlying cloud applications are technologically sophisticated.

Future research should validate the framework using real small-enterprise environments across different industries and cloud architectures. Longitudinal studies could assess whether improvements in integration and control maturity reduce audit effort, shorten exception-detection time, improve control reliability, or influence audit quality. Field research should also examine cost barriers, auditor competencies, cybersecurity concerns, application programming interface stability, dependence on technology providers, and the extent to which small enterprises can adopt continuous auditing incrementally. Such evidence would help transform continuous auditing from a predominantly technology-oriented concept into a practical and proportionate assurance capability for cloud-based small enterprises.

References

1. Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems, 20*, 26–37. https://doi.org/10.1016/j.accinf.2016.01.003
2. Lins, S., Schneider, S., & Sunyaev, A. (2018). Trust is good, control is better: Creating secure clouds by continuous auditing. *IEEE Transactions on Cloud Computing, 6*(3), 781–795. https://doi.org/10.1109/TCC.2016.2522411
3. Zadeh, A. H., Akinyemi, B. A., Jeyaraj, A., & Zolbanin, H. M. (2018). Cloud ERP systems for small-and-medium enterprises: A case study in the food industry. *Journal of Cases on Information Technology, 20*(4), 53–70.
4. Abu-Musa, A. A. (2005). Investigating the perceived threats of computerized accounting information systems. *Journal of American Academy of Business, 7*(1), 9–15.

5. Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, *1*(1), 1–21.
6. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems, 22*(2), 195–214.
7. Alles, M. G., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems, 7*(2), 137–161.
8. Bumgarner, N., & Vasarhelyi, M. A. (2015). Continuous auditing—A new view. *Continuous Auditing: Theory and Application*, 1–19.
9. Chan, D. Y., Chiu, V., & Vasarhelyi, M. A. (2018). Continuous auditing: Theory and application. *Emerald Publishing*.
10. Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems, 24*(1), 91–112.
11. Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons, 29*(2), 439–449.
12. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory, 36*(4), 1–27.
13. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting, 13*(2), 1–20.
14. Deloitte. (2017). *Internal Audit Analytics: A Practical Guide to Continuous Auditing and Monitoring*. Deloitte Insights.
15. ICAEW. (2018). *How to Audit the Cloud*. Institute of Chartered Accountants in England and Wales. The guidance emphasizes cloud security, supplier management, risk management, and regulatory compliance in cloud auditing.
16. Maex, S., & Shi, W. (2020). The audit implications of cloud computing. *Accounting Horizons, 34*(4), 1–31. https://doi.org/10.2308/HORIZONS-19-166
17. Al-Hiyari, A., Ismail, S., & Kolsi, R. H. (2020). Internal audits in the digital era: Opportunities, risks and challenges. *EuroMed Journal of Business, 15*(2), 205–217. https://doi.org/10.1108/EMJB-07-2019-0097
18. Mancini, D., Vaassen, E. H. J., & Dameri, R. P. (2017). Accounting information systems for decision making. *Springer*.
19. Rikhardsson, P., & Dull, R. (2016). Continuous auditing technology adoption and its impacts in small businesses. *International Journal of Accounting Information Systems, 20*, 26–37.
20. Jayeola, O., Sidek, S., Abd Rahman, A., Bali Mahomed, A. S., & Hu, J. (2022). Cloud computing adoption in small and medium enterprises (SMEs): A systematic literature review and directions for future research. *International Journal of Business and Society*.