JOURNAL OF MULTIDISCIPLINARY RESEARCH AND INTEGRATED SCIENCES

Volume 1, Issue 1, 2026 | **Article ID:** JMRIS-2026-004 | **Pages:** 31-40 | **Article Type:** Structured Evidence Synthesis

Received: 16-08-2026 | **Revised:** 19-08-2026 | **Accepted:** 22-08-2026 | **Published:** 24-08-2026

Cybersecurity Awareness and Intention to Adopt Cloud-Based Financial Systems Among Small and Medium-Sized Enterprises: An Extended Technology Acceptance Model Evidence Synthesis

Elena Hartwell1*

1 Department of Management, London School of Economics and Political Science, London, United Kingdom

***Corresponding author:** Elena Hartwell, Department of Management, London School of Economics and Political Science, London, United Kingdom | elenajacob1215@gmail.com

ABSTRACT

Background: Cloud-based financial systems can provide small and medium-sized enterprises (SMEs) with lower infrastructure costs, real-time access to accounting information, scalability and improved financial visibility. Adoption decisions, however, are influenced not only by perceived usefulness and ease of use but also by concerns about cybersecurity, privacy, trust and organizational preparedness. **Objective:** To synthesize evidence available on SME adoption of cloud-based financial systems and to evaluate cybersecurity awareness as an extension to the Technology Acceptance Model (TAM). **Methods:** A structured evidence synthesis was conducted using peer-reviewed literature from high-ranking journals in accounting information systems, information systems, cybersecurity, innovation and management. Studies were eligible when they examined cloud accounting, cloud ERP or cloud-computing adoption in SMEs, or when they directly assessed SME cybersecurity awareness, preparedness or risk perception. Because no eligible pre-2026 study identified in the review directly estimated the complete extended-TAM model proposed here, no synthetic path coefficients were generated. **Results:** The evidence consistently supported perceived benefit or relative advantage as an important adoption driver, while ease of use, organizational readiness, compatibility, external support and security factors showed context-dependent effects. A 2024 cloud-accounting study in SMEs found that employee capability, organizational resources, management support and technological factors influenced willingness to adopt cloud-based accounting. A 2025 study of 172 Vietnamese companies found security/privacy and system integration to be significant predictors of cloud-accounting adoption. In parallel, cybersecurity studies showed substantial SME knowledge gaps: UK SMEs often perceived attack probability as low despite expecting high impact, while Western Australian SMEs reported lack of funding and uncertainty about where to begin as major barriers to preparedness. **Conclusion:** Cybersecurity awareness is a credible extension to TAM because it changes how decision-makers interpret perceived risk, trust and the effort required to use cloud financial systems safely. The most defensible model is not that awareness simply increases adoption; rather, adequate awareness converts undifferentiated fear into informed trust and makes organizational readiness more actionable. SMEs should therefore combine usability and business-value evaluation with targeted cybersecurity capability development before adoption.

Keywords: cybersecurity awareness; cloud accounting; cloud financial systems; small and medium-sized enterprises; Technology Acceptance Model; perceived usefulness; perceived ease of use; cloud adoption

1. Introduction

Cloud-based financial systems have become an important component of SME digital transformation. Cloud accounting, online payroll, cloud enterprise-resource-planning modules and financial dashboards allow organizations to access data remotely, automate routine transactions and reduce dependence on locally maintained infrastructure. These features are particularly attractive to smaller firms because they can obtain capabilities that would otherwise require substantial information-technology investment.

The Technology Acceptance Model remains one of the most widely used frameworks for explaining technology adoption. Davis proposed that perceived usefulness and perceived ease of use shape attitudes and behavioral intention toward a system [1]. Later technology-acceptance research confirmed that performance expectations, effort expectations and contextual factors remain central across different technologies and organizations [2].

Cloud financial systems add a distinctive complication because the object being moved into the cloud is highly sensitive. Accounting platforms contain banking information, payroll data, invoices, tax records, supplier details, customer information and credentials. Consequently, adoption intention can be influenced by the same factors that make the technology attractive and by the perceived consequences of losing control over data or access.

Accounting-specific research demonstrates that adoption is already a multi-factor decision. Ma et al. found that small and medium accounting practices considered perceived benefits,

organizational readiness and external pressure when adopting cloud-based client accounting [3]. Mujalli et al. similarly examined SMEs using a framework integrating Technology-Organization-Environment factors with TAM and found that technology, organizational resources, employee capability and management conditions influenced willingness to adopt cloud-based accounting [4].

Recent business evidence further shows that security is not a peripheral consideration. Nguyen Phu et al. analyzed 172 Vietnamese companies and identified security/privacy and system integration as significant predictors of cloud-accounting adoption [5]. At the broader cloud-computing level, Kumar et al. found that relative advantage, cost-effectiveness, compatibility and external environmental support significantly influenced cloud adoption among 405 SME owners and managers, and that adoption subsequently improved organizational agility and financial performance [6].

The cybersecurity literature, however, suggests that SME decision-makers may not possess sufficiently calibrated risk perceptions. Wilson et al. reported that UK SMEs perceived the likelihood of several cyberattacks as relatively low despite believing their consequences would be high [7]. Chidukwani et al. found that Western Australian SMBs faced major barriers including lack of funds, limited knowledge of where to begin and poor familiarity with relevant cybersecurity frameworks [8]. Arroyabe et al. similarly identified information asymmetry and underinvestment in cybersecurity among UK SMEs [9].

These findings create a theoretical problem for conventional TAM. Security concern can reduce intention because a technology appears risky, but cybersecurity awareness may also increase adoption by enabling managers to distinguish manageable risk from uncontrolled risk. An uninformed SME may avoid cloud technology out of fear, while another uninformed SME may adopt it without adequate safeguards. A more useful model must therefore distinguish awareness from concern.

The present paper synthesizes the adoption and cybersecurity evidence and proposes an extended TAM in which cybersecurity awareness shapes perceived security, trust and cyber risk. The objective is to clarify how SMEs can adopt cloud-based financial systems without treating either technology acceptance or cybersecurity preparedness as a separate managerial problem.

2. Methods

This study used a structured evidence-synthesis design. Peer-reviewed literature published on or before 31 December 2025 was considered. The principal organizational population was SMEs, MSMEs and small or medium accounting practices. Studies of larger organizations were included only when they contributed directly to cloud-accounting security or financial-management mechanisms that were transferable to SMEs.

Search concepts combined cloud accounting, cloud financial systems, cloud computing, cloud ERP, SMEs, MSMEs, Technology Acceptance Model, TAM, perceived usefulness, perceived ease of use, cybersecurity awareness, security concern, cyber risk, trust, organizational readiness and adoption intention. Priority was given to journals in accounting information systems, information management, cybersecurity, technology and innovation management.

Evidence was included when it informed at least one component of the proposed model: perceived usefulness or relative advantage, perceived ease of use or complexity, organizational readiness, security/privacy, cybersecurity awareness or preparedness, trust/risk, or behavioral intention to adopt cloud technology. Purely technical cloud-security studies without an organizational adoption component were excluded from the core synthesis.

The findings were synthesized narratively because the eligible studies used different theoretical models, populations, dependent variables and statistical methods. Some measured actual adoption, others adoption intention, resilience, financial performance or cybersecurity preparedness. A meta-analysis of path coefficients would therefore create false comparability.

The extended-TAM relationships were classified as established, context-dependent or proposed. Established relationships were those consistently supported by TAM or multiple cloud-adoption studies. Context-dependent relationships were supported in some SME settings but not others. Proposed relationships were theoretically supported by adjacent cybersecurity evidence but had not been directly estimated as part of the complete model by the evidence cutoff.

The evidence-selection and extended-TAM framework is summarised in Table 1.

3. Results

The evidence supported the continuing relevance of TAM but showed that SME cloud-financial-system adoption cannot be explained by usefulness and ease of use alone. Perceived benefits and relative advantage were recurring drivers, while security, organizational readiness, integration and external support frequently changed the strength or direction of adoption intention.

Ma et al. studied cloud-based client accounting in eight small and medium accounting practices [3]. Adoption decisions were shaped by perceived benefits, partner-program benefits, organizational readiness and external pressure. Importantly, firms reported post-adoption changes in service mix and client relationships, indicating that cloud systems are not only technical replacements but can alter the business model of financial-service delivery.

Mujalli et al. extended cloud-accounting adoption research by combining technology and organizational variables with TAM among SME accountants [4]. Their model emphasized relative advantage, compatibility, complexity, organizational resources, employee capability and senior management support. The study is relevant to the present model because employee capability can be interpreted as a bridge between nominal system accessibility and the organization's capacity to use that system safely and effectively.

Nguyen Phu et al. provided 2025 evidence from 172 Vietnamese listed companies [5]. Security/privacy and system integration significantly predicted cloud-accounting adoption, while adoption and related integration/cost variables were associated with better financial-management outcomes. Although the sample was not limited to SMEs, the results confirm that security perceptions can function as an adoption determinant rather than merely an implementation issue.

Kumar et al. examined 405 SME owners and managers and found that relative advantage, cost-effectiveness, compatibility and external environment support significantly influenced cloud-computing adoption [6]. Adoption improved organizational agility and financial performance. Complexity was not significant in their final model, illustrating that ease-of-use-related constructs can become less decisive once cloud tools reach a baseline level of usability or when other organizational conditions dominate.

The principal evidence informing the extended model is summarised in Table 2.

3.1 Cybersecurity awareness and risk calibration

The cybersecurity literature indicates that awareness should not be represented as the inverse of security concern. Concern is an emotional or evaluative response to perceived risk, whereas awareness includes knowledge of threats, controls, responsibilities and realistic exposure. An SME can therefore be highly concerned but poorly aware, or highly aware and relatively confident because risks are understood and controlled.

Wilson et al. provide empirical support for this distinction [7]. Their UK respondents often rated the likelihood of network compromise, data theft or encryption as low while simultaneously anticipating substantial consequences if such events occurred. Preventive measures were generally perceived as affordable and effective, yet self-efficacy was weaker for areas such as mobile-device security and phishing. This configuration reflects incomplete risk calibration rather than simply high or low concern.

Chidukwani et al. similarly found that SMBs lacked knowledge of where to begin implementing cybersecurity and were unfamiliar with relevant regulations and frameworks [8]. Such deficits can influence technology acceptance in two directions. They may increase avoidance because the cloud seems opaque, or they may increase unsafe adoption because decision-makers underestimate shared-responsibility requirements.

Arroyabe et al. found that cybersecurity implementation among UK SMEs was affected by information asymmetry and myopia, with neither prior incidents nor their impacts necessarily driving optimal implementation [9]. This supports the argument that experience alone does not guarantee informed security behavior. Awareness must be deliberately developed.

The extended Technology Acceptance Model for secure cloud-financial-system adoption in SMEs is illustrated in Figure 1.

3.2 Proposed extended-TAM relationships

The proposed relationships and evidentiary status are presented in Table 3.

3.3 Organizational readiness and implementation capability

The evidence also shows that adoption intention and implementation readiness should not be conflated. A manager may perceive a cloud platform as useful and easy to use but lack secure identity management, backup procedures, access governance or staff training. In financial systems, this gap can create a situation in which successful adoption increases operational exposure.

Al Hadwer et al.'s systematic review of cloud-technology adoption identified top-management support, relative advantage, complexity and competitive pressure among the most important organizational factors across the literature [11]. This reinforces the view that TAM should be nested within a wider organizational context for SME research.

Bada and Nurse argued that SME cybersecurity education should be practical, targeted and connected to real organizational needs rather than generic awareness messaging [10]. For cloud financial systems, this means that cybersecurity training should address concrete adoption tasks: multifactor authentication, phishing-resistant access, role separation, privileged accounts, backup/recovery, secure data export, vendor responsibility and incident escalation.

The secure adoption pathway for cloud-based financial systems in SMEs is illustrated in Figure 2.

4. Discussion

The main conclusion of this synthesis is that cybersecurity awareness is best modeled as a risk-calibration capability within technology acceptance rather than as a simple positive or negative attitude toward security. This distinction resolves an apparent contradiction in cloud-adoption research. Security concern can inhibit adoption in some studies, while security and privacy can positively predict adoption in others. The difference may depend on whether respondents interpret security as an uncontrolled threat or as a valued property of a trustworthy system.

Traditional TAM focuses on whether users believe a system will improve performance and whether it can be used without excessive effort. These variables remain important, but cloud financial systems create a third question: whether the user understands enough about digital risk to evaluate the technology accurately. Without that capability, usefulness and ease may lead to adoption that is behaviorally attractive but operationally unsafe.

The proposed model therefore positions cybersecurity awareness upstream of trust and perceived risk. Awareness can increase recognition that cloud systems face credential theft, phishing and third-party risk, which might initially increase perceived threat. At the same time, awareness allows users to evaluate encryption, multifactor authentication, access controls, backup arrangements, certifications and incident procedures. As knowledge improves, generic uncertainty can be replaced by differentiated judgment.

This model predicts a non-linear relationship between awareness and adoption. Very low awareness may produce either complacency or avoidance. Intermediate awareness may temporarily increase perceived risk as threats become visible. Higher capability should permit a more balanced assessment of provider controls and organizational readiness. For this reason, future empirical studies should not assume that greater cybersecurity awareness must always have a direct positive coefficient on adoption intention.

The SME context magnifies the importance of this pathway. Smaller firms often rely on owners, general managers or external service providers for technology decisions. They may not have a chief information-security officer, dedicated accounting-systems team or internal audit function. Chidukwani et al.'s finding that many SMBs do not know where to begin is therefore directly relevant to cloud-financial-system adoption [8].

The evidence also suggests that cloud adoption can generate real business value. Ma et al. observed changes in service provision and client relationships after cloud-accounting adoption [3], while Kumar et al. linked cloud adoption to organizational agility and financial performance [6]. These potential gains mean that cybersecurity should not become a blanket argument against cloud migration. The goal is secure enablement rather than risk elimination.

Service providers have a corresponding responsibility. Cloud financial systems targeted at SMEs should make secure behavior easy through default multifactor authentication, clear role-based access, understandable activity logs, straightforward backup/export processes and concise explanations of shared responsibility. From a TAM perspective, security controls that are difficult to configure may increase effective complexity and reduce perceived ease of use. Security-by-design therefore supports both protection and acceptance.

For researchers, the next step is an empirical extended-TAM study using SME decision-makers who are actively considering

or recently adopting cloud financial systems. Cybersecurity awareness should be measured as knowledge/capability, not merely fear. Perceived security, trust and cyber risk should be separate constructs, and organizational readiness should be modeled as a contextual factor. Such a design would allow direct testing of whether awareness moderates or mediates the security-intention relationship.

The evidence-informed implementation and research framework is presented in Table 4.

Strengths and Limitations

The strength of this synthesis is that it connects two research streams that are often treated separately: technology acceptance of cloud financial systems and cybersecurity capability in SMEs. It also avoids representing security concern and cybersecurity awareness as the same construct and clearly labels the proposed awareness pathways as hypotheses rather than established path coefficients.

The principal limitation is the absence of a single pre-2026 Q1 study directly estimating the complete proposed model among SME cloud-financial-system adopters. The evidence is therefore triangulated from cloud accounting, general cloud adoption and SME cybersecurity studies. Definitions of SMEs differ across countries, and studies measure actual adoption and behavioral intention differently. Some accounting studies focus on accountants or listed firms rather than owner-managed SMEs. Finally, the rapid evolution of cloud platforms and security controls may change the relative importance of specific acceptance factors.

Future Research

Future research should survey SME owners, finance managers and accountants at different stages of adoption and estimate the extended model using covariance-based SEM or PLS-SEM with adequate measurement validation. A useful design would distinguish objective cybersecurity knowledge from self-rated awareness and test perceived security, trust and cyber risk as separate mediators.

Longitudinal studies should also examine whether pre-adoption awareness predicts safer actual use after migration. Adoption intention is only an intermediate outcome; the stronger test is whether informed adopters implement multifactor authentication, role separation, secure backups and incident-response practices while also achieving expected financial-process benefits.

Conclusion

Cloud-based financial systems can provide substantial efficiency, accessibility and performance benefits for SMEs, but adoption decisions involve more than usefulness and ease of use. Evidence available through 2025 shows that security/privacy, organizational readiness, employee capability, relative advantage and external support shape cloud adoption, while SME cybersecurity research demonstrates persistent gaps in threat awareness and implementation knowledge. Cybersecurity awareness should therefore be incorporated into technology-acceptance research as a capability that calibrates perceived risk and trust. The resulting extended TAM predicts that secure adoption is most likely when decision-makers understand both the business value of the system and the controls required to manage cloud risk. For SMEs, the practical implication is that cybersecurity training is not an activity to conduct after cloud migration. It is part of the adoption decision itself.

Declarations

Funding: No external funding was received for this structured evidence synthesis.

Conflict of Interest: The authors declare no conflict of interest.

Ethical Approval: Not applicable because no new human-participant data were collected.

Consent to Participate: Not applicable.

Data Availability: All findings were derived from the cited peer-reviewed literature available through 31 December 2025.

References

1. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 1989;13(3):319-340. doi:10.2307/249008.
2. Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: toward a unified view. MIS Q. 2003;27(3):425-478. doi:10.2307/30036540.
3. Ma D, Fisher R, Nesbit T. Cloud-based client accounting and small and medium accounting practices: adoption and impact. Int J Account Inf Syst. 2021;41:100513. doi:10.1016/j.accinf.2021.100513.
4. Mujalli A, Wani MJG, Almgrashi A, Khormi T, Qahtani M. Investigating the factors affecting the adoption of cloud-based accounting in SMEs. J Open Innov Technol Mark Complex. 2024;10(2):100314. doi:10.1016/j.joitmc.2024.100314.
5. Nguyen Phu G, Hoang Thi T, Tran Nguyen Bich H. The impact of cloud computing technology on cloud accounting adoption and financial management of businesses. Humanit Soc Sci Commun. 2025;12:851. doi:10.1057/s41599-025-05190-3.
6. Kumar J, Rani V, Rani G, Rani M. Is cloud computing a game-changer for SME financial performance? Unveiling the mediating role of organizational agility through PLS-SEM. Bus Process Manag J. 2025;31(6):2433-2452. doi:10.1108/BPMJ-10-2024-1004.
7. Wilson M, McDonald S, Button D, McGarry K. It won't happen to me: surveying SME attitudes to cyber-security. J Comput Inf Syst. 2023;63(2):397-409. doi:10.1080/08874417.2022.2067791.
8. Chidukwani A, Zander S, Koutsakis P. Cybersecurity preparedness of small-to-medium businesses: a Western Australia study with broader implications. Comput Secur. 2024;145:104026. doi:10.1016/j.cose.2024.104026.
9. Arroyabe MF, Arranz CFA, Fernandez De Arroyabe I, Fernandez de Arroyabe JC. Exploring the economic role of cybersecurity in SMEs: a case study of the UK. Technol Soc. 2024;78:102670. doi:10.1016/j.techsoc.2024.102670.
10. Bada M, Nurse JRC. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Inf Comput Secur. 2019;27(3):393-410. doi:10.1108/ICS-07-2018-0080.
11. Al Hadwer A, Tavana M, Gillis D, Rezania D. A systematic review of organizational factors impacting cloud-based technology adoption using Technology-Organization-Environment framework. Internet Things. 2021;15:100407. doi:10.1016/j.iot.2021.100407.
12. Oliveira T, Thomas M, Espadanal M. Assessing the determinants of cloud computing adoption: an analysis of the manufacturing and services sectors. Inf Manag. 2014;51(5):497-510. doi:10.1016/j.im.2014.03.006.
13. Hoong Y, Rezania D. Balancing talent and technology: navigating cybersecurity and privacy in SMEs. Telemat Inform Rep. 2024;15:100151. doi:10.1016/j.teler.2024.100151.

Table 1. Evidence-selection and extended-TAM framework

Domain	Included evidence	Excluded evidence	Analytical purpose
Publication period	Published through 31 December 2025	2026 onward	Maintains chronological fit for Volume 6
Organization	SMEs, MSMEs and small/medium accounting practices	Large-enterprise evidence without SME relevance	Preserves target context
Technology	Cloud accounting, cloud ERP and cloud-based financial information systems	Non-financial consumer cloud use	Focuses on sensitive business systems
Acceptance constructs	Usefulness, ease of use, compatibility, readiness, trust, security, risk	Technology attitudes unrelated to adoption	Maps evidence to extended TAM
Cybersecurity constructs	Awareness, preparedness, threat appraisal, capability, information gaps	Purely technical attack-detection studies	Explains risk interpretation
Synthesis	Narrative comparison and conceptual integration	Pooled structural coefficients	Avoids combining non-equivalent models

Table 2. Principal evidence informing the extended model

Study	Context/design	Primary constructs	Main finding	Extended-TAM relevance	Caution
Davis, 1989 [1]	Technology acceptance	Perceived usefulness; perceived ease of use	Both constructs shape technology acceptance	Core TAM pathways	Individual-level foundational model
Ma et al., 2021 [3]	Eight small/medium accounting practices	Benefits, readiness, external pressure	These factors shaped cloud-client-accounting adoption	Adds readiness and interorganizational context	Qualitative sample
Mujalli et al., 2024 [4]	SME accountants	TAM plus TOE variables	Employee capability, resources and technology/management factors influenced adoption	Supports capability as external TAM input	Country/context specific
Nguyen Phu et al., 2025 [5]	172 Vietnamese companies; SEM	Security/privacy, integration, cost-benefit	Security/privacy and integration predicted cloud-accounting adoption	Direct support for security as adoption antecedent	Not SME-only
Kumar et al., 2025 [6]	405 SME owners/managers; PLS-SEM	Relative advantage, cost, compatibility, external support	Significant effects on cloud adoption; adoption improved performance	Shows value and context pathways	General cloud computing, not accounting only
Wilson et al., 2023 [7]	85 UK SMEs	Threat and coping appraisal	Attack likelihood often perceived as low despite high expected impact	Demonstrates risk-perception calibration problem	Cybersecurity rather than cloud adoption
Chidukwani et al., 2024 [8]	Western Australian SMB survey	Awareness, preparedness, NIST practices	Funding and knowledge gaps were major barriers	Supports cybersecurity-awareness construct	Different regulatory environment
Arroyabe et al., 2024 [9]	240 UK SMEs	Cybersecurity implementation and information asymmetry	Knowledge gaps and underprovision produced suboptimal security investment	Explains why awareness affects readiness	Economic outcome, not TAM

Table 3. Proposed relationships and evidentiary status

Relationship	Expected direction	Evidence status	Rationale	Representative evidence
Perceived usefulness -> adoption intention	Positive	Established	Cloud systems are more acceptable when managers expect efficiency, access or financial-management benefits	Davis [1]; Ma et al. [3]; Kumar et al. [6]
Perceived ease of use -> adoption intention	Positive	Established but context-dependent	Lower effort supports acceptance, although mature cloud tools may reduce variance in ease	Davis [1]; cloud-adoption literature [4,6]
Cybersecurity awareness -> perceived security/trust	Positive	Proposed, strongly supported mechanistically	Knowledge of controls enables informed confidence rather than undifferentiated fear	Bada & Nurse [10]; Chidukwani et al. [8]
Cybersecurity awareness -> perceived cyber risk	Calibrating rather than simply negative	Proposed	Awareness can increase recognition of threats while reducing uncertainty about mitigation	Wilson et al. [7]; Arroyabe et al. [9]
Perceived security/trust -> adoption intention	Positive	Supported	Sensitive financial data require confidence in platform and provider controls	Nguyen Phu et al. [5]
Perceived cyber risk -> adoption intention	Negative when risk is viewed as unmanaged	Supported conceptually/contextually	Expected losses reduce willingness to migrate sensitive financial processes	Cloud and cybersecurity evidence [5,8,9]
Organizational readiness -> adoption intention	Positive	Established external factor	Skills, resources and management support allow intention to become feasible action	Ma et al. [3]; Mujalli et al. [4]
Vendor/external support -> adoption intention	Positive	Context-dependent	SMEs depend more heavily on providers and external expertise	Al Hadwer et al. [11]; Kumar et al. [6]

Table 4. Evidence-informed implementation and research framework

Stage	SME question	Acceptance construct	Cybersecurity requirement	Suggested measure	Expected benefit
Needs assessment	Which financial processes should move to the cloud?	Perceived usefulness	Classify data and critical processes	Expected time/cost/access benefit	Avoid technology-first adoption
Usability assessment	Can staff perform routine tasks reliably?	Perceived ease of use	Secure defaults and role design	Task completion, support burden	Maintains acceptance without weakening controls
Awareness assessment	Do decision-makers understand major cloud risks?	Cybersecurity awareness	Phishing, MFA, backups, permissions, provider responsibility	Knowledge/scenario score	Improves risk calibration
Provider evaluation	Are controls transparent and credible?	Perceived security/trust	Encryption, certifications, logging, SLA, recovery	Trust/security scale plus vendor checklist	Converts generic concern into evidence-based trust
Pilot	Does the system work in the real organization?	Attitude/intention	Training, least privilege, incident procedures	User acceptance plus security observations	Tests socio-technical fit
Post-adoption	Are value and risk outcomes improving?	Actual use/continuance	Audit logs, access reviews, recovery tests	Usage, incidents, financial-process performance	Supports continuous improvement

Figure 1. Extended Technology Acceptance Model for secure cloud-financial-system adoption in SMEs

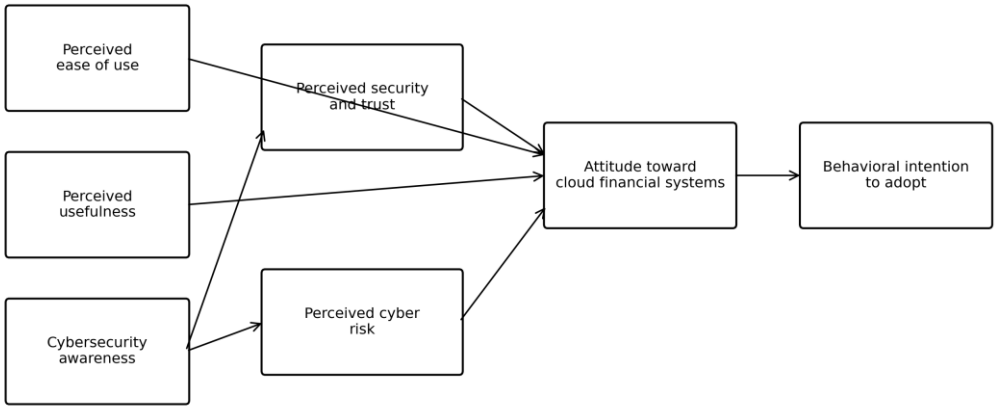

Figure 1. Extended Technology Acceptance Model for secure cloud-financial-system adoption in SMEs.

Solid pathways summarize evidence-supported relationships; cybersecurity awareness is presented as a proposed risk-calibration extension requiring direct empirical testing.

Figure 2. Secure adoption pathway for cloud-based financial systems in SMEs

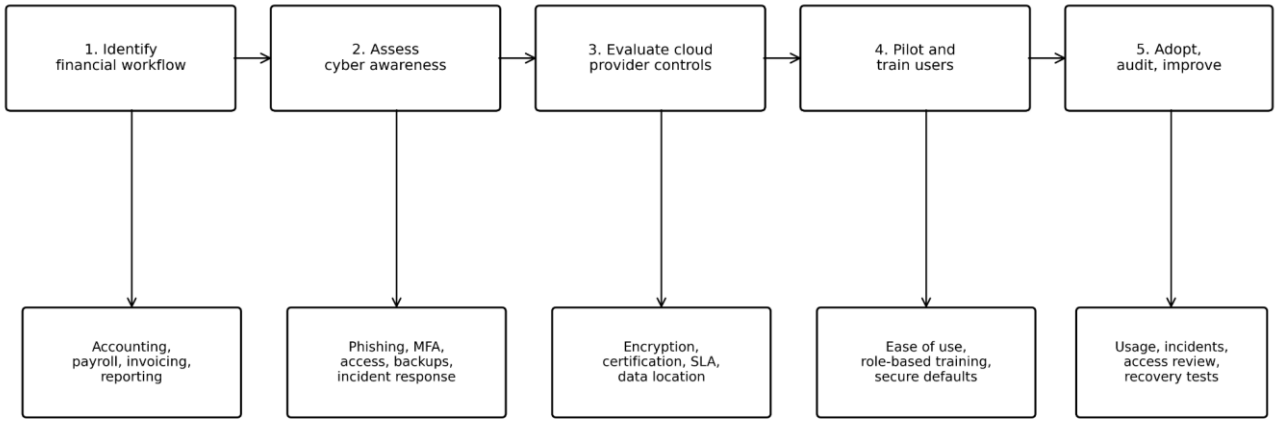

Figure 2. Secure adoption pathway for cloud-based financial systems in SMEs.

Secure adoption requires both acceptance and capability: a system that is useful but poorly understood can create avoidable cyber risk.

How to cite: Hartwell E (2026). Cybersecurity Awareness and Intention to Adopt Cloud-Based Financial Systems Among Small and Medium-Sized Enterprises: An Extended Technology Acceptance Model Evidence Synthesis. Journal of Multidisciplinary Research and Integrated Sciences, 6(1).