MRS Journal of Accounting and Business Management
ISSN *(Online) 3049-1460*
Vol-3, Iss-5 (May-2026)
Journal homepage: https://mrspublisher.com/journals

Cybersecurity Risks in Cloud-Based Accounting Information Systems

Dr. Sultana Rajahmad Pathan*

Ph D in Commerce

Received: 06 / 04 / 2026	Accepted: 13 / 05 / 2026	Published: 25 / 05 / 2026

Abstract: The migration of accounting information systems (AIS) from on-premise infrastructure to cloud-based platforms has transformed the way organisations record, process, store, and report financial data. Cloud-based accounting systems offer significant benefits, including cost efficiency, scalability, real-time data access, and simplified system maintenance. However, this transition also introduces a distinct and evolving set of cybersecurity risks that threaten the confidentiality, integrity, and availability of financial information. This paper examines the principal cybersecurity risks associated with cloud-based accounting information systems, including data breaches, ransomware attacks, insider threats, misconfigured cloud environments, insecure application programming interfaces, and third-party vendor vulnerabilities. It further explores the regulatory and compliance dimensions of cloud accounting security, including data protection regulations and audit implications, and reviews prevailing risk mitigation frameworks such as encryption, multi-factor authentication, access control, and continuous monitoring. Drawing on a synthesis of academic literature, industry reports, and regulatory guidance, the paper argues that effective cybersecurity risk management in cloud-based accounting environments requires an integrated approach combining technical controls, governance mechanisms, and organisational awareness. The paper concludes with recommendations for accounting professionals, auditors, and organisational leadership seeking to strengthen the security posture of cloud-based financial information systems.

Keywords: *Cybersecurity, cloud computing, accounting information systems, data breach, financial reporting, risk management, information security.*

Cite this article: Pathan, S. R. (2026). Cybersecurity Risks in Cloud-Based Accounting Information Systems. *MRS Journal of Accounting and Business Management, 3(5),58-61.*

Introduction

Accounting information systems have historically been maintained on organisation-owned servers and localised networks, with financial data stored within physically controlled premises. The emergence of cloud computing has fundamentally altered this paradigm, enabling organisations to outsource the storage, processing, and management of financial data to third-party cloud service providers. Cloud-based accounting information systems, delivered through Software-as-a-Service (SaaS) platforms and similar models, have gained widespread adoption across organisations of varying size, driven by their capacity to reduce infrastructure costs, enable remote and real-time access to financial data, and offer scalable computing resources that adjust to organisational needs.

Despite these advantages, the shift towards cloud-based accounting introduces a fundamentally different risk landscape compared to traditional on-premise systems. Financial data, by its nature, is highly sensitive and represents an attractive target for malicious actors seeking financial gain, competitive advantage, or reputational disruption of targeted organisations. The distributed and multi-tenant architecture of cloud environments, combined with reliance on third-party providers for security controls, introduces vulnerabilities that differ substantially from those associated with traditional, organisation-controlled information systems. Furthermore, the interconnected nature of cloud services, often integrating multiple third-party applications through application programming interfaces, expands the potential attack surface available to malicious actors.

This paper examines the cybersecurity risks associated with cloud-based accounting information systems and evaluates the mechanisms available to mitigate these risks. The paper is structured as follows: Section 2 outlines the objectives of the study; Section 3 reviews the relevant literature on cloud computing and accounting information systems security; Section 4 describes the research methodology; Section 5 presents a detailed examination of the principal cybersecurity risks; Section 6 discusses regulatory and audit implications; Section 7 reviews risk mitigation strategies and frameworks; Section 8 offers recommendations; and Section 9 concludes the paper.

Objectives of the Study

This study is guided by the following objectives:

- To identify and categorise the principal cybersecurity risks associated with cloud-based accounting information systems.
- To examine the implications of these risks for financial data integrity, confidentiality, and regulatory compliance.
- To evaluate the role of external auditors and internal control functions in addressing cloud-related cybersecurity risks.

- To review existing technical and organisational frameworks for mitigating cybersecurity risks in cloud accounting environments.
- To propose practical recommendations for organisations adopting or operating cloud-based accounting information systems.

Review of Literature

Cloud Computing and Accounting Information Systems

Cloud computing is generally understood as a model for enabling on-demand network access to a shared pool of configurable computing resources, including servers, storage, and applications, that can be rapidly provisioned with minimal management effort. Within the accounting domain, cloud-based platforms have enabled the delivery of accounting functionality as a service, allowing organisations to access general ledger, accounts receivable and payable, payroll, and financial reporting modules through web-based interfaces rather than locally installed software.

The literature identifies several deployment models relevant to accounting information systems, including public cloud, private cloud, and hybrid cloud arrangements, each presenting distinct trade-offs between cost efficiency and control over security configurations. Public cloud deployments, characterised by shared infrastructure across multiple tenants, offer the greatest cost efficiency but require organisations to place substantial trust in the security practices of the cloud service provider. Private and hybrid deployments offer greater control but at correspondingly higher cost, and are more commonly adopted by larger organisations with more stringent regulatory or security requirements.

Cybersecurity Risk in Financial Information Systems

Financial information systems have long been recognised in the literature as high-value targets for cyberattacks, given the direct financial gain achievable through the manipulation or theft of financial data, and the reputational and regulatory consequences associated with breaches of financial data confidentiality. Prior research on information systems security has established a taxonomy of risk that distinguishes between threats to confidentiality, such as unauthorised data access; threats to integrity, such as unauthorised alteration of financial records; and threats to availability, such as denial-of-service conditions that prevent access to financial systems during critical reporting periods.

The migration of these systems to cloud environments introduces additional considerations relating to the shared responsibility model of cloud security, whereby security obligations are divided between the cloud service provider, who is typically responsible for the security of the underlying cloud infrastructure, and the client organisation, who remains responsible for securing data, user access, and application-level configurations within that infrastructure. Misunderstanding or inadequate management of this shared responsibility boundary has been identified in the literature as a recurring source of security failures in cloud-hosted systems, including accounting platforms.

Regulatory and Audit Perspectives

The accounting and auditing literature has increasingly addressed the implications of cloud computing for internal control frameworks and external audit procedures. Auditing standards addressing information technology general controls require auditors to assess the design and operating effectiveness of controls over financial reporting systems, a task complicated by the reduced visibility that client organisations and their auditors have over infrastructure managed by third-party cloud providers. Service organisation control reports, commonly used to provide assurance over the controls maintained by cloud service providers, have become an important reference point for auditors seeking to evaluate cloud-related risks within the context of financial statement audits.

Regulatory frameworks governing data protection, such as those addressing the processing and cross-border transfer of personal and financial data, impose additional compliance obligations on organisations utilising cloud-based accounting systems, particularly where such systems involve the storage of customer or employee financial data across multiple jurisdictions. Non-compliance with these frameworks carries not only reputational risk but also the potential for substantial financial penalties, further elevating the stakes associated with cybersecurity failures in cloud accounting environments.

Methodology

This paper adopts a conceptual and analytical research design, drawing on a synthesis of peer-reviewed academic literature, industry security reports, and regulatory and professional standards guidance relating to cloud computing, information systems security, and accounting information systems. The analysis categorises identified risks according to established information security taxonomies distinguishing threats to confidentiality, integrity, and availability, and further examines these risks through the lens of the shared responsibility model that characterises cloud service arrangements.

The paper does not present primary empirical data collected through surveys or case studies; rather, it offers a structured synthesis intended to consolidate dispersed literature into a coherent risk framework relevant to accounting practitioners, auditors, and organisational decision-makers. Future research employing case-study analysis of security incidents within cloud-based accounting environments, or survey-based assessment of organisational security practices, would provide valuable empirical extension of the conceptual analysis presented here.

Principal Cybersecurity Risks in Cloud-Based Accounting Information Systems

Data Breaches and Unauthorised Access

Data breaches involving unauthorised access to financial records represent one of the most significant risks associated with cloud-based accounting systems. Such breaches may arise from compromised user credentials, exploitation of software vulnerabilities, or inadequate access control configurations within the cloud environment. Given that accounting systems typically store highly sensitive information, including bank account details, tax identification numbers, payroll records, and transactional data, unauthorised access carries substantial financial and reputational consequences, including potential exposure to fraud, identity theft, and regulatory penalties.

Ransomware and Malware Attacks

Ransomware attacks, in which malicious actors encrypt organisational data and demand payment for its release, pose a particularly acute threat to cloud-based accounting systems, given

the operational disruption caused by the inability to access financial records during critical reporting or transaction processing periods. While cloud service providers typically implement backup and redundancy mechanisms that can mitigate the impact of ransomware, organisations that fail to configure adequate backup retention policies or that store backup credentials within the same compromised environment remain vulnerable to significant data loss and operational disruption.

Insider Threats

Insider threats, arising from employees or contractors with legitimate access to accounting systems, represent a persistent risk that is not eliminated by migration to cloud platforms. Cloud-based systems, by virtue of enabling remote access from a broader range of devices and locations, may in some cases increase the difficulty of monitoring and detecting anomalous insider activity compared to traditional, physically bounded on-premise systems. Insider threats may manifest as deliberate fraud, such as unauthorised alteration of financial records for personal gain, or as inadvertent security failures, such as the accidental exposure of sensitive data through misconfigured sharing settings.

Misconfigured Cloud Environments

Misconfiguration of cloud infrastructure has been consistently identified across industry security reports as one of the leading causes of data exposure incidents in cloud environments generally, and this risk extends directly to cloud-based accounting systems. Common misconfigurations include overly permissive access controls, publicly accessible storage repositories containing sensitive financial data, and inadequate encryption of data at rest or in transit. Given the shared responsibility model underlying cloud security, responsibility for correct configuration of these controls typically rests with the client organisation, making organisational awareness and technical competence critical determinants of security outcomes.

Insecure Application Programming Interfaces (APIs)

Cloud-based accounting platforms frequently integrate with third-party applications, including payment processors, banking platforms, and enterprise resource planning systems, through application programming interfaces that facilitate automated data exchange. Insecure API implementations, characterised by inadequate authentication, insufficient input validation, or excessive data exposure, represent a growing vector for cyberattacks, as they may allow malicious actors to intercept, manipulate, or extract financial data flowing between integrated systems without directly compromising the core accounting platform itself.

Third-Party and Vendor Risk

The reliance of cloud-based accounting systems on third-party service providers introduces vendor-related risks that extend beyond the direct control of the client organisation. These risks include the security practices of the primary cloud service provider, as well as those of any subcontracted infrastructure or service providers within the broader supply chain. Security incidents affecting a cloud service provider or its subcontractors can simultaneously impact numerous client organisations utilising the same shared infrastructure, a phenomenon that has been documented in several large-scale security incidents affecting cloud-hosted business applications.

Denial-of-Service and Availability Risks

Availability risks, including distributed denial-of-service attacks that overwhelm cloud infrastructure with malicious traffic, threaten the continuous accessibility of accounting systems required for time-sensitive financial operations such as payroll processing, invoice issuance, and regulatory reporting deadlines. While large cloud service providers typically maintain substantial infrastructure redundancy to mitigate such attacks, smaller providers or those serving niche accounting software markets may possess more limited capacity to withstand large-scale availability attacks.

Regulatory and Audit Implications

The adoption of cloud-based accounting systems carries significant implications for regulatory compliance and external audit procedures. Data protection regulations in numerous jurisdictions impose specific obligations regarding the security, storage location, and cross-border transfer of personal and financial data, requiring organisations to conduct due diligence on the data handling practices of their cloud service providers and, in many cases, to formalise these arrangements through data processing agreements. Failure to adequately address these obligations exposes organisations to regulatory penalties independent of any direct financial loss arising from a security incident.

From an audit perspective, the migration of accounting systems to cloud environments necessitates a re-evaluation of information technology general controls testing procedures, as auditors must assess controls that are, in significant part, implemented and maintained by an external service provider rather than the audited organisation itself. Service organisation control reports issued by independent auditors of the cloud service provider have become an increasingly important source of assurance in this context, although auditors must exercise judgement in assessing the scope, coverage period, and relevance of such reports to the specific systems and controls relevant to the financial statement audit.

Risk Mitigation Strategies and Frameworks

Technical Controls

A range of technical controls has been identified in the literature as effective in mitigating the cybersecurity risks associated with cloud-based accounting systems. Encryption of data both at rest and in transit reduces the risk of data exposure in the event of unauthorised access, while multi-factor authentication substantially reduces the risk of account compromise arising from stolen or weak credentials. Role-based access control, whereby user permissions are assigned according to job function and the principle of least privilege, limits the potential scope of both insider threats and externally compromised accounts. Continuous security monitoring and logging of system activity further enable the timely detection of anomalous behaviour indicative of a security incident in progress.

Governance and Organisational Measures

Beyond technical controls, effective cybersecurity risk management in cloud accounting environments requires robust governance mechanisms, including clearly defined information security policies, formal vendor risk assessment procedures prior to the selection of cloud service providers, and regular review of the shared responsibility arrangements governing the division of

security obligations between the organisation and its provider. Organisations are further advised to conduct periodic security audits and penetration testing of cloud-hosted accounting systems, subject to the terms of service agreements with their cloud providers, to proactively identify vulnerabilities before they can be exploited by malicious actors.

Employee Awareness and Training

Given the persistent role of human error and insider risk in cybersecurity incidents, organisational training programmes addressing secure password practices, recognition of phishing attempts, and proper handling of sensitive financial data represent an essential complement to technical and governance controls. Literature on information security culture suggests that organisations with strong security awareness cultures, reinforced through regular training and leadership commitment to security priorities, experience materially lower rates of security incidents attributable to human error compared to organisations lacking such cultures.

Recommendations

Based on the preceding analysis, the following recommendations are proposed for organisations operating or considering the adoption of cloud-based accounting information systems. First, organisations should conduct thorough due diligence of prospective cloud service providers, including review of available security certifications and service organisation control reports, prior to system adoption. Second, organisations should implement multi-factor authentication and role-based access control as baseline security measures across all cloud-based accounting system accounts, with particular emphasis on accounts possessing administrative or elevated privileges.

Third, organisations should establish clear internal accountability for cloud security configuration management, ensuring that responsibility for correctly configuring access controls, encryption settings, and data sharing permissions is explicitly assigned rather than assumed to be the sole responsibility of the cloud provider. Fourth, organisations should incorporate cloud-specific cybersecurity risk assessment into their broader enterprise risk management and internal audit programmes, rather than treating cloud security as a purely technical matter outside the scope of financial control evaluation. Finally, organisations should invest in ongoing employee security awareness training, recognising that technical controls alone are insufficient to address the human factors that continue to contribute significantly to cybersecurity incidents in cloud-based financial systems.

Conclusion

This paper has examined the principal cybersecurity risks associated with cloud-based accounting information systems, situating these risks within the broader context of the shared responsibility model that characterises cloud computing arrangements. The analysis identifies data breaches, ransomware attacks, insider threats, misconfigured cloud environments, insecure application programming interfaces, third-party vendor vulnerabilities, and availability attacks as principal categories of risk confronting organisations that rely on cloud-hosted financial systems. The discussion further highlights the regulatory and audit implications of these risks, underscoring the need for enhanced due diligence, revised audit procedures, and robust internal governance frameworks.

The paper concludes that effective cybersecurity risk management in cloud-based accounting environments cannot rely on technical controls alone but requires an integrated approach encompassing governance, vendor management, regulatory compliance, and organisational security culture. As cloud adoption within the accounting profession continues to expand, ongoing research into emerging threats, evolving regulatory requirements, and the effectiveness of specific mitigation strategies will remain essential to supporting the secure and reliable operation of cloud-based financial information systems.

References

1. American Institute of Certified Public Accountants. (2017). Reporting on an examination of controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy (SOC 2). AICPA.
2. Ali, O., Shrestha, A., Osmanaj, V., & Muhammed, S. (2021). Cloud computing technology adoption: An evaluation of key factors in local governments. Information Technology & People, 34(2), 666–703.
3. Alshare, K. A., Lane, P. L., & Miller, D. (2018). Business continuity management and information security in the cloud. Journal of Computer Information Systems, 58(2), 130–139.
4. European Union Agency for Cybersecurity. (2021). Cloud security for healthcare services. ENISA.
5. International Auditing and Assurance Standards Board. (2019). ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement. IFAC.
6. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372–386.
7. National Institute of Standards and Technology. (2011). NIST SP 800-145: The NIST definition of cloud computing. U.S. Department of Commerce.
8. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM Conference on Computer and Communications Security, 199–212.
9. Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2014). Cloud security auditing: Challenges and emerging approaches. IEEE Security & Privacy, 12(6), 68–74.
10. Verizon. (2023). 2023 data breach investigations report. Verizon Business.