

Cloud Adoption in Accounting Information Systems in Asia & SOC 2® Report – An Empirical Study on Industry’s Perspective

Anil K. Makhija*

ABSTRACT

Many business and technology organizations see cloud adoption and migrating existing systems to the cloud as an accelerator of digital transformation. The benefits of cloud adoption are perceived as increased scalability and cost reduction. At the same time, there are concerns about whether the information on cloud-based systems is secure and whether the privacy of the data in a cloud environment is at risk. This research brings out the industry’s perspective, both from an end-user perspective as well as IT transformation and IT procurement decision makers of accounting information systems and enterprise resource planning systems in Asia geography, on the preference for cloud-based or on-premise systems, top enablers for cloud adoption and importance of SOC 2® as an assurance for information security and data privacy concerns. The findings of this research indicate that decision-makers for IT transformation and IT procurement prefer cloud-based accounting information systems and enterprise resource planning systems over on-premise systems. Scalability, cost reduction, business agility, business continuity and disaster recovery, and enhanced collaboration are top enablers for cloud adoption. This research also indicates that the SOC 2® report is increasingly seen to address information security and data privacy concerns.

Keywords: SOC 2®; Trust services criteria; Information security; Data privacy; Cloud computing; Accounting Information Systems

INTRODUCTION

Migration to cloud-based systems and solutions has significantly increased in the last decade. Cloud adoption enables and accelerates organizations’ journey of digital transformation. There are significant benefits of cloud adoption ranging from cost reduction to scalability. There are also concerns about data privacy and information security for the data and information stored on cloud-based systems. To accelerate the digital journey, organizations continue to adopt the cloud and, at the same time, address security, privacy, and other concerns through various assurance mechanisms. Some assurance mechanisms are based on seeking ISO 27001 certifications focusing on information security. SOC 2® provides more comprehensive assurance as it covers principles related to security, availability, processing integrity, confidentiality, and privacy embodied in the trust services criteria (AICPA, 2021; Borangiu et al., 2019; Vasiljeva et al., 2017; Ulas, 2019).

This research aims to gather the industry’s perspective on their preference for cloud-based or on-premise

applications, top enablers for cloud adoption, and usage of SOC 2® report as an assurance mechanism. Industry practitioners from user organizations were asked to respond to a survey questionnaire. Those practitioners covered those in the role of end users in the user organizations and those involved in making decisions related to cloud adoption.

LITERATURE REVIEW

Accounting Information Systems help organizations collect, store, and record data related to business transactions of the organizations and process it into meaningful information that aids both strategic and operational management teams. Accounting Information Systems provide insights into the effectiveness and efficiency of organizational business processes and make data-driven decisions. An Accounting Information System consists of Transaction Processing System supporting, a General Ledger System & Financial Reporting System, and the Management Reporting System. When integrated with other systems of organizations, accounting information systems provide a holistic view to enable effective decision-making (Belfo & Trigo, 2013; Bhatt, 2001; Salehi et al., 2010; Soudani, 2012).

* Anil K. Makhija, B.E., PGDİM, MBA. Lecturer, CamEd Business School
Email: anil@cam-ed.com

The Accounting Information System's design significantly impacts the ability of the Accounting Information System to support its ability in strategic decision-making. Research has investigated the relationship of management control systems' effectiveness to design considerations (Chenhall, 2003).

Past research also establishes that if the design of the Accounting Information System is not appropriate, it can significantly negatively impact the firm's performance, in addition to the money and time spent on the design and implementation of the Accounting Information System itself (Boulianne, 2007). Another research study conducted on Small and Medium Sized Enterprises indicates that when the processing capability and capacity of an Accounting Information System match its requirements, reflecting the quality and appropriateness of the design of the Accounting Information System, the firm reflected a higher level of performance as well as more effective utilization of information technology by its managers (Ismail & King, 2005). Studies have indicated that the technology systems (specifically, enterprise resource planning systems) are easy to implement and institutionalize with a focus on standardization and integration. In contrast, business needs are shifting more towards agility and flexibility. As an extension of such studies, it can be stated that systems that are easier to create flexibility in implementation despite standardization in design will enable more alignment between business and technology priorities (Mancini et al., 2013).

Technological advances have led to how organizations acquire and use accounting information systems. Recent advances in cloud computing and its widespread adoption have profoundly impacted Accounting Information Systems delivery models. Research indicates that with many such accounting information systems being offered as part of enterprise resource planning software in a SaaS (Software as a Service) model, multiple organizations can have their accounting information systems within the same cloud, enabling faster electronic data interchange. There is also an overall cost reduction and increased flexibility due to pay-per-use pricing models. Research also indicates that while most of the cloud service providers implement state-of-the-art security solutions, there are risks of data loss, privacy, availability, and loss of intellectual property that are still inherent and shall be mitigated (Asatiani & Penttinen, 2015; Brandas et al., 2015).

The Internet has been revolutionizing both the technology and business space in an unprecedented manner. Technological advances have made the impact of the Internet revolution more profound and accelerated. One of the leading enablers in this has been Cloud Computing. Cloud computing services are delivered through service models such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). In an Infrastructure as a service model, the cloud provider provides the consumer organization's capability to process, store, network, and compute resources to the consumer organization. In the Platform as a service model, the cloud provider provides the cloud infrastructure (consisting of processing, storage, network, and compute resources) and the environment (consisting of programming languages and other related tools) over which consumer organizations can deploy the applications built by them or built for them by a third-party provider or providers. In the Software as a Service model, the cloud provider provides the running application to the consumer organization that they can use over the web (Puthal et al., 2015; Sunyaev, 2020).

The National Institute of Standards and Technology (NIST) classifies cloud deployment into private, public, community, and hybrid clouds. As the name suggests, a private cloud is exclusively used by the organization for which it is deployed. In the Public cloud, the cloud services are shared by a group of users. Community cloud is used to define scenarios where the cloud is shared by several organizations and/or groups that share a common mission or objective. A cloud deployment model that imbibes more than one of the above three deployment models is termed a hybrid cloud. Cloud adoption comes with its own set of benefits and risks. Benefits related to the lower overall cost of IT, lower initial investment in IT hardware and IT Infrastructure, scalability, and flexibility are expected when the cloud is adopted. The risks and issues related to cloud adoption revolve around data security, privacy, availability, and intellectual property exposure. While adopting the cloud, keeping information secure is of utmost importance. Security on the cloud consists of three significant dimensions of security: computer security, network security, and information security. Data security and privacy are the most prominent risk factors critical for cloud adoption decisions (Chou, 2015; Rao & Selvamani, 2015; Sun, 2018).

Exciting research on data breaches over 15 years, from 2000 to 2015, indicate that the risk of personal data breaches is taking alarming dimensions. This research indicates that such breaches can also lead to mass identity fraud. With an ever-increasing amount of data (and personal data) being used and stored by organizations, this risk is becoming predominant and concerning. The research proposes, amongst many aspects that need to be addressed, decentralization of IT systems in big organizations to stop/reduce the significant breach events and their cascading impact (Wheatley et al., 2016).

Another research on 9000 data breaches made public since 2005 shows that these data breaches led to the loss of 11.5 billion individual records. This study indicates that hacking breaches significantly impact the volume of stolen data among various kinds of breaches. The study also indicates that most such breaches are financially motivated and target, as a priority, the organizations that are least prepared to deal with such attacks. Another research study conducted over five years, from 2009 to 2014, indicated that external consequences of cybercrime are business disruption, equipment damage, information loss, and revenue loss. Another research evaluated the impact of 441 data breach announcements from 2005 to 2017. This research covered multiple industries, with the finance and insurance industry contributing 37.4 percent of total data breach announcements. Analysis done in this research demonstrated that the performance of the breached companies suffered in the quarter when such breaches were announced. Another research conducted through a laboratory experiment demonstrated that privacy is considered extremely important to build trust. Hence privacy violation leads to some erosion in the trust factor. However, security breaches have a direct impact on the actual behavior. Security breaches have a higher impact on actual decision-making. This research explains this finding to be in alignment with the “privacy paradox,” which suggests that people do not act according to their privacy concerns. This research highlights the importance of investment in security in order to address the mitigate the security risks faced by organizations across the world (Hammouchi et al., 2019; Hemphill & Longstreet, 2016; Juma’h & Alnsour, 2020; Nofer et al., 2014).

Several research studies have analyzed the trust barriers to cloud adoption. One of the research projects on data privacy and trust in cloud computing

identifies the predominant factors/risks that are inherent in and also drive the decision to adopt and migrate to the cloud. This research identifies privacy and security as essential challenges and barriers in cloud adoption for those considering and those already relying on the cloud. Another research on the barriers to cloud adoption indicated that perceived security is a significant factor driving cloud adoption. The research found it more of a cloud adoption driver than a barrier. Additionally, this research identified customer service and user-friendliness as barriers to cloud adoption. This research also indicates that information security is crucial when deciding on cloud adoption. Another study developed a model for cloud adoption and tested it on 149 Australian SMEs. The findings of this research indicated that SMEs were more focused on factors such as relative advantage, quality of service, and awareness, that help them gain advantages similar to the larger organizations. The risk factors related to security, privacy, and flexibility were less significant amongst the participating SMEs. The research also indicated that awareness of the technology landscape also impacts cloud adoption. One of the challenges with this research was that only 27.5 percent of the respondent organizations were using some cloud service. Another research was conducted to examine the factors affecting adopting cloud enterprise resource planning (ERP) in small and medium-sized developing countries. This research analyzed four contexts, namely diffusion of innovation context, technological context, organizational context, and environmental context. Technological context, in this research, consisted of technology readiness, security concerns, and technical barriers. The findings of this research indicated that technology readiness and technical barriers were significant factors, whereas security concerns were insignificant (AL-Shboul & Moh’d, 2018; Lynn et al., 2021; Senarathna et al., 2018; Townsend et al., 2020).

Despite all the challenges, cloud investment and adoption are growing. New vulnerabilities and threats to information assurance have also accompanied this growth. Cloud service providers have used various certifications and attestations to assure their clients utilizing third-party assessments and auditing their systems and internal controls. ISO 9001:2015 is one such leading certification focused on information security. SOC 2® - SOC for Service Organizations: Trust Services Criteria report, part of Systems and Organization Controls (SOC), is another such report. A type 1 report provides management’s description

of a service organization’s systems and the suitability of the design of controls. A type 2 report provides management’s description of a service organization’s systems and the suitability of design and operating effectiveness of controls. These are restricted-use reports (AICPA, 2021; Giulio et al., 2017).

CURRENT STATUS AND RESEARCH QUESTIONS

As evident from the above analysis, security and privacy are important considerations that some consider barriers to cloud adoption, while some research establishes them more as drivers for decisions regarding cloud adoption. Previous research does indicate that security and privacy have an impact on cloud adoption decisions. Despite all these concerns, there has been phenomenal growth in organizations leveraging the benefits of cloud adoption to reduce their overall technology cost and get the desired scalability to grow and diversify their businesses. To address these concerns, cloud service providers use certifications and attestation services to assure their client’s security and privacy. One of the leading attestations, SOC 2®, is based on Trust Services Criteria. Trust Services criteria include security, processing integrity, availability, confidentiality, and privacy. There has not been any research that provides insights into the industry’s perspective on what reports and certifications they consider to provide sufficient assurance to address their security and data privacy concerns, especially SOC 2®. Hence, in the context of accounting information systems and enterprise resource planning systems, this research aims to answer the following questions:

- (1) Is there a preference (amongst Accounting Information Systems user organizations) for an on- premise accounting information system over a cloud-based accounting information system (or vice versa)?
- (2) What would be (or are) the top enablers for their decisions to adopt a cloud-based accounting solution?
- (3) Have Accounting Information Systems user organizations used (or will consider using) SOC 2® for their cloud adoption decision?

RESEARCH METHODOLOGY

The research involved a questionnaire-based survey (conducted online) of end users of accounting information systems and those involved in decisions related to acquiring accounting information systems/ enterprise resource planning systems and decisions related to transformation through cloud adoption. The industry coverage was Banking & Financial Services covering both banking and insurance, Retail, Pharmaceuticals, and Manufacturing organizations. The geographic scope of the survey (based on responses received) was mainly Asia, some from North America (US & Canada), and very few from Europe.

The survey questionnaire was designed to gather insights on the following dimensions:

- Preference amongst end-users/decision makers for on-premise information systems versus cloud-based information systems (Usage-based or Perception-based)
- Factors considered necessary (by the decision makers) in driving the decisions for cloud adoption
- Perception about security and privacy concerns in an on-premise system versus a cloud-based system
- What certification/report/evidence is sought as an assurance that information stored on the cloud will be secured and data privacy will be ensured
- Their experience with cloud service providers when they have adopted a cloud-based information system

Out of 300 persons reached out to, the total number of responses received was 207. The distribution of the respondents’ geographic coverage, industry coverage, and roles category is shown in Tables 1, 2, and 3.

Table 1: Survey respondents – Geography

Geography	Count	% Distribution
Asia (including Australia)	165	80%
North America (US & Canada)	32	15%
Europe	10	5%
Total	207	100%

Table 2: Survey respondents – Industry

Industry	Count	% Distribution
Banking & Financial Services	29	14%
Retail	94	45%
Pharmaceuticals	37	18%
Manufacturing	47	23%
Total	207	100%

Table 3: Survey respondents – Role

Role	Count	% Distribution
End-user	140	68%
Decision Maker - Transformation/ Procurement	67	32%
Total	207	100%

RESULTS ANALYSIS

Preference analysis - On-premise versus Cloud-based Information Systems

From the survey responses, it is evident that from an end-user perspective, most of them are indifferent to whether the information systems are on-premise or cloud-based. From the remaining, the majority preferred on-premise compared to cloud-based information systems. This is summarized and reflected in Table 4.

Table 4: On-Premise versus Cloud-based – Preference analysis for end-users

On-Premise v/s Cloud-Based	Count	Percentage
Does not Matter	80	57%
On-premise	43	31%
Cloud-based	17	12%
Total	140	100%

Further, it is evident from the survey responses that from decision makers (both those involved with transformation responsibility and those entrusted with procurement decisions), most prefer cloud-based information systems, followed by on-premise options. Only a minor percentage (21 percent) of them are indifferent to whether it's on-premise or cloud-based information systems are on-premise or cloud-based. This is summarized and reflected in Table 5.

Table 5: On-premise versus Cloud-based – Preference analysis for decision makers (Transformation/procurement)

On-Premise v/s Cloud-Based	Count	Percentage
Does not Matter	14	21%
On-premise	16	24%
Cloud-based	37	55%
Total	67	100%

Top enablers for decisions on cloud-based accounting solution adoption

Based on survey responses, the top enablers for deciding whether to migrate to a cloud-based accounting solution were scalability, cost reduction, business agility, business continuity and disaster recovery, and enhanced collaboration. The response analysis is summarized in Table 6.

Table 6: Enablers for Cloud-based accounting solution adoption

Top Reasons	Percentage
Scalability	88%
Cost Reduction	81%
Business Agility	79%
Business Continuity & Disaster Recovery	70%
Enhanced Collaboration	67%
Other factors	59%

Usage of SOC 2® reports for cloud-based accounting solution adoption decisions

Based on survey responses of decision-makers involved in transformation and/or procurement decisions, 76 percent have used or considered using the SOC 2® report. An almost similar number of respondents (75 percent) mentioned that they are also using other certifications for getting assurance regarding their security and privacy concerns. The response analysis is summarized in Table 7.

Table 7: Summary of usage of SOC 2® report

Usage of SOC 2® reports	Count	Percentage
Used SOC 2® report	28	42%
Considering using SOC 2® report	23	34%
Used Other Certifications (with or without SOC 2® report)	50	75%
Not used SOC 2® report or any other certification	16	24%

CONCLUSION AND FUTURE WORK

Research findings indicate that since 80 percent of respondents were from Asia geography, many end-users (57 percent) are still determining whether their accounting information systems and/or enterprise resource planning systems are on-premise or cloud-based. Thirty-one percent of the respondents had a preference for cloud-based systems.

From the perspective of decision-makers – both those involved in transformation and those entrusted with responsibilities of IT procurement, there was a clear preference for cloud-based systems, with 55 percent responding in favor of cloud-based systems.

Regarding top enablers for deciding migration to cloud-based accounting information systems or enterprise resource planning systems, scalability, cost reduction, business agility, business continuity & disaster recovery were identified as top reasons and enablers.

Regarding information security and data privacy, most respondents (76 percent) mentioned using or considering the SOC 2® report. A similar number of respondents (75%) said they are also using other certifications.

The findings of the report indicate that adopting cloud-based solutions has gained significant preference among IT-related decision-makers in organizations. The benefits of scalability, cost reduction, business agility, business continuity, and disaster recovery are seen as very important and relevant. Information Security and data privacy did not come out as barriers to cloud adoption. However, assurance for information security and data privacy is being addressed by using reports such as SOC 2® report and other certifications. Further, SOC 2® is seen as becoming the leading mechanism to address information security and data privacy concerns.

One of the limitations of this research is that the majority of respondents are from Asia geography. Hence the results of this report reflect the Asian perspective only. Researchers shall conduct studies focusing on other geographies for a more global perspective. Another essential aspect that can be addressed in future research is to gain insights and understand the industry's perspective on the relative importance of each of the principle of trust services criteria: security, availability, processing integrity, confidentiality, and privacy.

REFERENCES

- AICPA. (n.d.). *Soc 2® - SOC for service organizations: Trust services criteria*. AICPA. <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html>.
- AL-Shboul, Moh'd Anwer (2018). Towards better understanding of determinants logistical factors in SMEs for cloud ERP adoption in developing economies. *Business Process Management Journal*, 01, 0004. doi:10.1108/BPMJ-01-2018-0004
- Asatiani, A., & Penttinen, E. (2015). Managing the move to the cloud – Analyzing the risks and opportunities of cloud-based accounting information systems. *Journal of Information Technology Teaching Cases*, 5(1), 27–34. doi:10.1057/jittc.2015.5
- Belfo, F., & Trigo, A. (2013). Accounting information systems: Tradition and future directions. *Procedia Technology*, 9, 536–546. doi:10.1016/j.protcy.2013.12.060
- Bhatt, G. D. (2001). Knowledge management in organizations: Examining the interaction between technologies, techniques, and people. *Journal of Knowledge Management*, 5(1), 68–75. doi:10.1108/13673270110384419
- Borangiu, T., Trentesaux, D., Thomas, A., Leitão, P., & Barata, J. (2019). Digital transformation of manufacturing through cloud services and resource virtualization. *Computers in Industry*, 108(65), 150–162. doi:10.1016/j.compind.2019.01.006
- Boulianne, E. (2007). Revisiting fit between AIS design and performance with the analyzer strategic-type. *International Journal of Accounting Information Systems*, 8(1), 1–16. doi:10.1016/j.accinf.2006.12.001
- Brandas, C., Megan, O., & Didraga, O. (2015). Global perspectives on accounting information systems: Mobile and cloud approach. *Procedia Economics and Finance*, 20, 88–93. doi:10.1016/s2212-5671(15)00051-9
- Chenhall, R. H. (2003). Management control systems design within its organizational context: Findings from contingency-based research and directions for the future. *Accounting, Organizations and Society*, 28(2-3), 127–168. doi:10.1016/s0361-3682(01)00027-7

- Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces*, 38, 72–77. doi:10.1016/j.csi.2014.10.001
- Giulio, C. D., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R., & Bashir, Masooda N. (2017). IT security and privacy standards in comparison: Improving FedRAMP authorization for cloud service providers. *17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Madrid. doi:10.1109/CCGRID.2017.137
- Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & Koutbi, M. E. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, 151, 1004–1009. doi:10.1016/j.procs.2019.04.141
- Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society*, 44, 30–38. doi:10.1016/j.techsoc.2015.11.007
- Ismail, N. A., & King, M. (2005). Firm performance and AIS alignment in Malaysian SMEs. *International Journal of Accounting Information Systems*, 6(4), 241 – 259. doi:10.1016/j.accinf.2005.09.001
- Juma'h, Ahmad H.; Alnsour, Yazan (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, 28(2), 275–301. doi:10.1108/ijaim-01-2019-0006
- Lynn, T., Mooney, J. G., van der Werff, L., & Fox, G. (Eds.). (2021). *Data Privacy and Trust in Cloud Computing. Palgrave Studies in Digital Business & Enabling Technologies*. doi:10.1007/978-3-030-54660-1
- Mancini, D., Vaassen, E. H. J., & Dameri, R. P. (2013). Trends in Accounting Information Systems. *Accounting Information Systems for Decision Making*, 1–11. doi:10.1007/978-3-642-35761-9_1
- Mancini, D., Vaassen, E. H. J., & Dameri, R. P. (2013). Trends in Accounting Information Systems. *Accounting Information Systems for Decision Making*, 1–11. doi:10.1007/978-3-642-35761-9_1
- Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). *The Economic Impact of Privacy Violations and Security Breaches. Business & Information Systems Engineering*, 6(6), 339–348. doi:10.1007/s12599-014-0351-3
- Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015). *Cloud Computing Features, Issues, and Challenges: A Big Picture. 2015 International Conference on Computational Intelligence and Networks*. doi:10.1109/cine.2015.31
- Rao, R. V., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science*, 48, 204–209. doi:10.1016/j.procs.2015.04.171
- Salehi, M., Rostami, V., & Mogadam, A. (2010). Usefulness of Accounting Information System in Emerging Economy: Empirical Evidence of Iran. *International Journal of Economics and Finance*, 2(2). doi:10.5539/ijef.v2n2p186
- Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., & Salzman, S. (2018). Factors That Influence Adoption of Cloud Computing: An Empirical Study of Australian SMEs. *Australasian Journal of Information Systems*, 22. doi:10.3127/ajis.v22i0.1603
- Soudani, S. N. (2012). The Usefulness of an accounting information system for effective organizational performance. *International Journal of Economics and Finance*, 4(5). doi:10.5539/ijef.v4n5p136
- Sun, X. (2018). Critical security issues in cloud computing: A survey. *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, Omaha, NE, USA, 216–221. doi: 10.1109/BDS/HPSC/IDS18.2018.00053
- Sunyaev, A. (2020). *Internet computing: Principles of distributed systems and emerging Internet-based technology*. Springer Cham.
- Townsend, M., Wimmer, H., & Du, J. (2020). Barriers and drivers to adoption of cloud infrastructure services: A security perspective. *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, - Vancouver, BC, Canada (9-12 September 2020), 1–7. doi:10.1109/iemtronics51293.2020.9216342
- Ulas, D. (2019). *Digital transformation process and SMEs. Procedia Computer Science*, 158, 662–671. doi:10.1016/j.procs.2019.09.101

- Vasiljeva, T., Shaikhulina, S., & Kreslins, K. (2017). Cloud computing: Business perspectives, benefits and challenges for small and medium enterprises (Case of Latvia). *Procedia Engineering*, 178, 443–451. doi:10.1016/j.proeng.2017.01.087
- Wheatley, S., Maillart, T., & Sornette, D. (2015). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, 89(1). doi:10.1140/epjb/e2015-607 54-4