World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:4, 2022

Governance, Risk Management, and Compliance Factors Influencing the Adoption of Cloud Computing in Australia

Tim Nedyalkov

Abstract**—**A business decision to move to the cloud brings fundamental changes in how an organization develops and delivers its Information Technology solutions. The accelerated pace of digital transformation across businesses and government agencies increases the reliance on cloud-based services. Collecting, managing, and retaining large amounts of data in cloud environments make information security and data privacy protection essential. It becomes even more important to understand what key factors drive successful cloud adoption following the commencement of the Privacy Amendment Notifiable Data Breaches (NDB) Act 2017 in Australia as the regulatory changes impact many organizations and industries. This quantitative correlational research investigated the governance, risk management, and compliance factors contributing to cloud security success. The factors influence the adoption of cloud computing within an organizational context after the commencement of the NDB scheme. The results and findings demonstrated that corporate information security policies, data storage location, management understanding of data governance responsibilities, and regular compliance assessments are the factors influencing cloud computing adoption. The research has implications for organizations, future researchers, practitioners, policymakers, and cloud computing providers to meet the rapidly changing regulatory and compliance requirements.

Keywords**—**Cloud compliance, cloud security, cloud security governance, data governance, privacy protection.

I. Introduction

CLOUD computing has been transforming businesses and government agencies at an unprecedented pace. The growth and development of different cloud service models deliver business-supporting technology more efficiently than ever before [1]. Organizations that move from capital to operational expenditures save on infrastructure. A majority of companies have a multi-cloud strategy combining different service delivery models and vendors [2]. It enables organizations to embrace the latest technology capabilities easily. In many cases, cloud services enable innovation with flexible and scalable on-demand workloads. "Cloud-first initiatives" for both government agencies and the private sector in Australia have accelerated the broad adoption of cloud computing, resulting in appreciable portions of organizations' data now being cloud-based [3].

In July 2019, Capital One, the fifth largest consumer bank in the U.S. with $28 billion in revenue in 2018, disclosed that the bank had sensitive customer data of over 106 million customers accessed by an external party. Capital One was one of the first banks in the world to invest in digital transformation by migrating its on-premises data center to a cloud computing environment. The investigation of the Capital One incident showed that the bank failed to implement proper security for its cloud-based environment [4]. Data breaches have shown that companies worldwide were not well-suited to use and manage the security of new cloud computing environments. Therefore, key stakeholders should ensure proper governance and compliance requirements exist to support the organizational capabilities of addressing the latest technologies so that cybersecurity becomes a strategic business enabler. It is even more important to understand what fundamental factors drive successful cloud adoption following the commencement of the Privacy Amendment NDB Act 2017 in Australia as the regulatory changes impact many organizations and industries. The problem compelling this research is that the current studies within the Information Security (IS) domain do not adequately consider what governance, risk management, and compliance factors contribute to cloud security success within an organizational context after the commencement of the NDB scheme in Australia. The lack of understanding of the factors makes IS programs less effective, less efficient, and less enabling compared to when the factors and their interrelations are known. Furthermore, without this solid understanding, it is difficult for organizations and decision-makers to state the benefits of their IS programs accurately and consistently [5], as well as to ensure optimal resource utilization for future activities [6].

Prior research by Senarathna et al. [7] on cloud security in Australia included the participation of Small and Medium-Sized Enterprises (SMEs) via a quantitative survey method. Their study was limited to assessing only cloud privacy, cloud security, and cloud adoption for SMEs. The study does not address issues such as trust, user behavior, and technological issues, including, reliability, encryption, data rights, and transparency studied by Tomas et al. [8]. A study by Ali et al. [9] identifies and explores the critical factors associated with IS requirements of cloud services only within the Australian regional local government context. The gaps in the previous research and the legislative changes in Australia provide an opportunity to explore and demonstrate the relevant factors influencing the adoption of cloud computing in a wider context.

Tim Nedyalkov was with the University of Fairfax, VA, USA, now with the Commonwealth Bank of Australia (e-mail: tim4ned@gmail.com).

There is very little understanding of what makes a cloud adoption successful within an organization. Limited research focuses on understanding the expectations from governance, risk management, and compliance areas, and how they impact decision-makers after the commencement of the NDB scheme.

The primary aim of this study is to understand the current research topics and identify the future directions for cloud computing security for Australian organizations after the introduction of the latest data privacy regulations by the NDB scheme. It includes governance, risk management, and compliance perspectives. This study utilized a quantitative design method to address the problem area.

II. Background and Research Questions

A. *Significance of the Study*

Enterprises often resist adopting cloud computing, typically due to a lack of thorough understanding of the technology and how to successfully incorporate it within their organizations. Companies that move to cloud environments always experience challenges in protecting information. The existing literature indicated that cloud computing environments could introduce significant security issues to organizations' information [10], [11]. In the meantime, data security and privacy protection compliance requirements, such as the NDB scheme and the Australian Prudential Regulation Authority (APRA) CSP 234 IS regulation, have been introduced [12], [13]. This research considers the newly introduced laws and regulations while understanding the key factors impacting the adoption of cloud computing.

The results of this research could contribute new knowledge to businesses, future researchers, policymakers, and practitioners in various domains, including education, healthcare, government, entertainment, and emerging economic sectors. The results and findings demonstrate the importance of understanding and assessing the relevant factors while seeking to adopt cloud computing. Furthermore, the findings can assist in the evaluation existing cloud environments in terms of relevant cyber security considerations. The results support decision-makers in establishing improved cloud security requirements, which could lead to less reported compliance violations and a higher contribution of cloud computing to the overall quality of service and organizational IS program management.

B. *Nature of the Study*

The quantitative approach for this study incorporates a correlational, explanatory design. Quantitative research conceptualizes reality in terms of variables, measures the variables, and studies the relationships between them. The design indicates how the variables align conceptually concerning each other, which outlines the strategy behind the research. According to Creswell [14], it provides a resourceful way to control many unrelated variables that could differ between the selected groups. It allowed researchers to test theories and expectations that predict the results from the relating variables. Quantitative research provides an opportunity to create purpose statements, research questions, and hypotheses that were specific, measurable, and observable. It includes collecting numeric data from a large number of people, analyzing trends, comparing variables using statistical analysis, and comparing results against the prior research [15]. According to Thorndike [16], an association of direct proportion exists between sample size and the total number of variables. The study suggested that an informal approach requires 10 responses per variable, and a modifier of 50 added to the total to assure the reliability of smaller sample sizes. Expressed as an equation, this approach yields the following: $N \geq (10 \text{ x } V) + 50$. N defines the minimum acceptable number of responses and V includes the number of variables in a study. It suggests that a minimum of 75 participants in the selected problem provides statistically significant data to support research.

C. *Research Questions and Hypothesis*

Cloud services bring opportunities to accelerate business through its ability to deploy and scale resources quickly, maintain low-cost service delivery, and high reliability. While the adoption of cloud computing continues to surge, security concerns show no signs of decreasing. According to McAfee Cloud Adoption and Risk Report [3], 91% of cybersecurity professionals have extreme-to-moderate concerns about cloud security. Aligning enterprise risk management practices with organizational goals and benefits of cloud computing help to identify the weaknesses as well as the opportunities for improvement [17]. Therefore, it is essential to understand the key factors that lead to effective governance, risk management, and compliance practices of cloud computing environments.

A prior study by Ali et al. [9] found that an organization's selection and adoption of cloud services rely on assessing the technical complexities in terms of data security and risk mitigation practices. Additional researchers including Al-Ruithe et al. [18], Gangwar [19] and Subashini & Kavitha [20] have examined the adoption of IS in cloud environments, primarily focused on security effectiveness, reliability, cost-effectiveness, and organizational needs. The current literature review provided an opportunity to study the factors, such as regulatory, and compliance implications, which have not been used by IS practitioners during the selection and implication processes related to cloud computing. This study aimed to understand the factors influencing the adoption of cloud computing. The dependent variable is an organization's risk appetite towards the adoption of cloud computing. The three independent variables were (1) cybersecurity roles and responsibilities in an organization, (2) data security and privacy protection, (3) regulatory and compliance requirements. An assessment of these independent variables evaluated the factors affecting the adoption of cloud computing by organizations.

D. *Conceptual Framework*

The quantitative nature of the research focuses on studying the hypotheses, which helps obtain measures on the variables from observations [15]. Fig. 1 depicts the synthesized view of the independent and dependent variables of this study.

Open Science Index, Computer and Information Engineering Vol:16, No:4, 2022 publications.waset.org/10012500.pdf

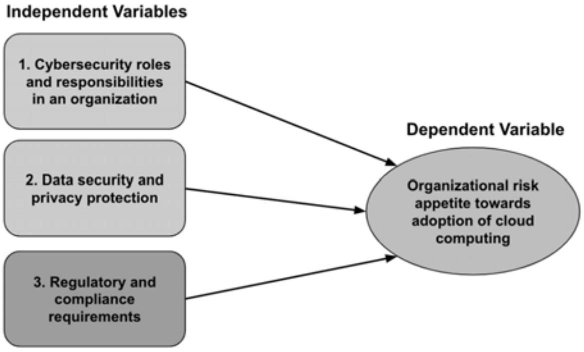
Independent Variables
1. Cybersecurity roles and responsibilities in an organization
2. Data security and privacy protection
3. Regulatory and compliance requirements
Dependent Variable
Organizational risk appetite towards adoption of cloud computing

Fig. 1 Conceptual Framework

From the background research and conclusions of the reviewed literature [21], it appears that the cloud computing industry continued to evolve. Organizations consider assessing and mitigating the risks of cloud computing to be increasingly crucial. Given the broad nature of risks and challenges associated with cloud computing to date, this study suggests a high-level decision-making framework that helped determine the factors that could lead to the adoption of cloud computing. The high-level decision-making framework depicted in Fig. 2 shows the alignment between the decision factors and the study areas. It represented a categorized view of the hypothesized list of the potential constraining or enabling decision factors selected for analysis applicable to the adoption of cloud computing. The holistic decision-making framework is built upon the study of Brandis et al. [22] that provides compliance efforts in cloud computing infrastructures.

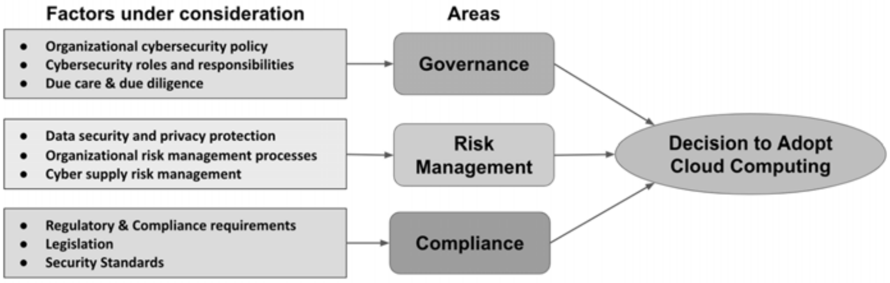
Factors under consideration
Areas
Organizational cybersecurity policy
Cybersecurity roles and responsibilities
Due care & due diligence
Governance
Data security and privacy protection
Organizational risk management processes
Cyber supply risk management
Risk Management
Regulatory & Compliance requirements
Legislation
Security Standards
Compliance
Decision to Adopt Cloud Computing

Fig. 2 Holistic Decision-making Framework

The framework considers governance factors such as organizational cybersecurity policy, cybersecurity roles and responsibilities, due care, and due diligence. Risk management factors assessed data security and privacy considerations, cyber supply risk management for cloud computing, and their value to an organization. Managing data security and privacy risks includes a complex process that requires the involvement of all levels of an organization, inclusive of the top and middle management, and teams implementing the cloud services [23]. The compliance area examined the impact of laws and regulatory requirements, such as the NDB scheme reporting introduced in 2018 [13].

III. Study Methodology

A. Research Approach

This quantitative study incorporated a correlational, exploratory design. The quantitative research evaluated problems by generating numerical data, which helped to test hypotheses about phenomena, and described the problems through a description of trends or an assessment of relationships between variables [24]. A quantitative method depended on tests, questionnaires, rating scales, and measures. The quantitative research design included analyzing trends, relating variables using statistical analysis, and interpreting results by comparing them with the past research [15]. This quantitative study aimed to test broad explanations of factors related to the adoption of cloud computing that predict results from the relevant variables. It justified the research problem driven by regulatory changes in Australia and creates a need for testing the hypotheses of the study. This approach helped assess the findings by using standard evaluation criteria and structures, which leads to an objective and unbiased approach [25]. For the context of this study, three independent variables incorporated nominal data type which led to measurable outcomes. The hypothesis testing and analysis employed .05 level of significance methodology suggested by Creswell and Creswell [24]. If the p-value is less than or equal to .05, the null hypothesis is rejected.

B. Data Collection Tool

An online web-based survey was used to collect the data for further analysis. Conducting anonymous surveys with close-ended questions relies on the participants' integrity that no one would inadvertently participate in the survey more than once [26]. The participants signed an informed consent before participating in the survey, which clarified the expectations of data collection and maintenance. The nature of this study aimed to include data from individuals that work in various fields, including telecommunications, IT, finance, healthcare, cybersecurity, and etc. Furthermore, data analysis techniques were incorporated to analyze the data collected through this research.

C. Research Questions

This study addressed four research questions relevant to governance, risk management, and compliance for cloud computing. The research questions test the hypotheses with a correlation between the independent and dependent variables.

Open Science Index, Computer and Information Engineering Vol:16, No:4, 2022 publications.waset.org/10012500.pdf

The research questions included the hypotheses and their respective null hypotheses. The null hypotheses aimed to identify if there is no difference between the selected groups' independent variables in terms of the dependent variable for the research site [24].

- RQ1: What are the critical governance, risk management and compliance factors influencing the adoption of cloud computing?

The question outlined the factors identified by the literature review in the area [27], [28]. For the context of the study, critical factors determine if a majority of the participants agree with the question of the relevant area [25].

The study used the following hypotheses:

- H1: There are critical factors influencing the adoption of cloud computing.
- $H_0$1: There are no critical factors influencing the adoption of cloud computing.

- RQ2: Do the concerns of data security and privacy protection restrain the management's decision in adopting cloud computing?

Multiple researchers identified the factors under consideration as necessary [18], [29]. This study tested the following hypotheses:

- H2: The concerns of data security and privacy protection restrain the management's decision in adopting cloud computing.
- $H_0$2: The concerns of data security and privacy protection do not restrain the management's decision in adopting cloud computing.

- RQ3: Do regulatory and compliance requirements negatively affect the management's decision in adopting cloud computing?

Previous research highlighted that regulatory and compliance as the primary factors for cloud computing adoption [13], [30]. The hypotheses under consideration included:

- H3: Regulatory and compliance requirements negatively impact the management's decision in adopting cloud computing.
- $H_0$3: Regulatory and compliance requirements do not negatively impact the management's decision in adopting cloud computing.

- RQ4: Do the existing laws and regulations in Australia protect the privacy, access, and confidentiality in the cloud environments?

The area has become increasingly important because of the recent regulatory changes [31], [32]. This study considered the following hypotheses:

- H4: The existing laws and regulations in Australia protect the privacy, access, and confidentiality in the cloud environments.
- $H_0$4: The existing laws and regulations in Australia do not protect the privacy, access, and confidentiality in the cloud environments.

D. Measurement Instruments

The analysis of the collected data helped prove or reject the null hypotheses of the study. The *p*-values of each correlation were compared to the .05 level of significance of the study. If the *p-value* is less than or equal to .05, the null hypothesis is rejected [24]. Hypothesis testing and analysis of the demographic's information was performed through Chi-Square, cross-tabulation, and regression analysis. Chi-square is a post hoc method for hypothesis testing to determine the strength of the relationships between the study variables.

This study used a self-designed survey to measure the organizational risk appetite toward adopting cloud services, which contributed to assessing the governance, risk management, and compliance factors that influence cloud computing adoption. Table I represents the operational measures for the three independent variables, which the previous research has presented as the essential factors for adopting cloud computing [7], [33]. It includes the types of variables, their conceptual definitions, data type, and scale of measurement utilized by the survey. The data types and scales of measurement include concepts applied by previous research and help outline the most relevant ways to ensure measurements of the variables.

TABLE I
OPERATIONAL MEASURE OF VARIABLES

Conceptual Definition	Variable Type	Operational Measure	Data Type	Scale
Organizational risk appetite towards the adoption of cloud computing.	Dependent	Analysis of independence	Ordinal	1 to 5
Cybersecurity roles and responsibilities in an organization.	Independent	Likert Scale	Ordinal	1 to 5
Data security and privacy protection.	Independent	Likert Scale	Ordinal	1 to 5
Regulatory and compliance requirements.	Independent	Likert Scale	Ordinal	1 to 5
Years of experience.	Demographic/ Moderator	Number of years	Ratio	1 of 6
Job role.	Demographic/ Moderator	Type of role	Nominal	1 of 10
Organization size.	Demographic/ Moderator	Size of the organization served	Ratio	1 of 6
Industry.	Demographic/ Moderator	Industry served	Nominal	1 of 10
Region/territory.	Demographic/ Moderator	Location	Nominal	1 of 9

IV. RESULT AND FINDINGS

A. Representation of the Collected Data

The results from the conducted survey and data analysis were divided into three segments. The first summarized the representation of the sample, demographic characteristics, industries, organizational size, and the relationships that support the objectives of this study. The second provided exploratory data analysis results to determine what (if any) relationships exist between the demographic data and the dependent variable. The last segment outlined the results of hypothesis testing performed on the independent and dependent variables.

Demographic analysis was carried out to identify the possible trends in data to determine what influence demographics could have on the research results. The total number of collected responses from the survey is 104. Information Technology (26.90%) is the primary industry that the respondents belong to, followed by Professional Services (19.20%) and Finance (12.50%). These industries account for 58.60% of total responses of the survey. Fig. 3 depicts the overall representation of industries.

A majority of the respondents have 51 to less than 1,000 (54.46%) employees in their organizations, followed by 1,001 to less than 5,000 (25.74%). Fig. 4 depicts the overall representation of organizations size. Almost half of the population sample (47.52%) of the respondents have 5 to less than 10 years' experience in IS. 35.64% of them have less than 5 years' experience. Fig. 5 depicts the overall distribution of years of experience in IS.

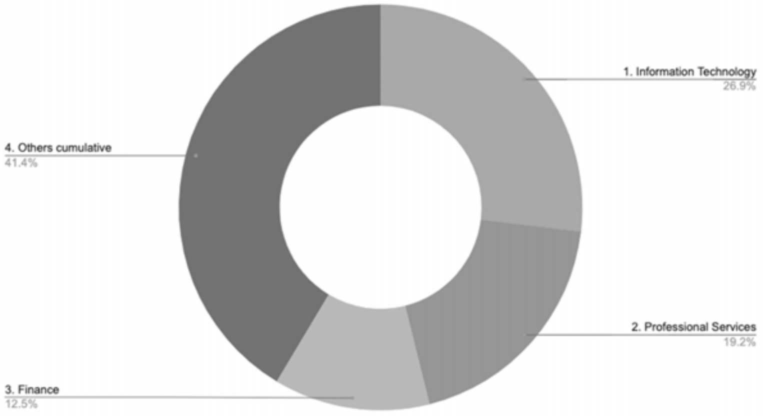

Fig. 3 Overall Industries Representation

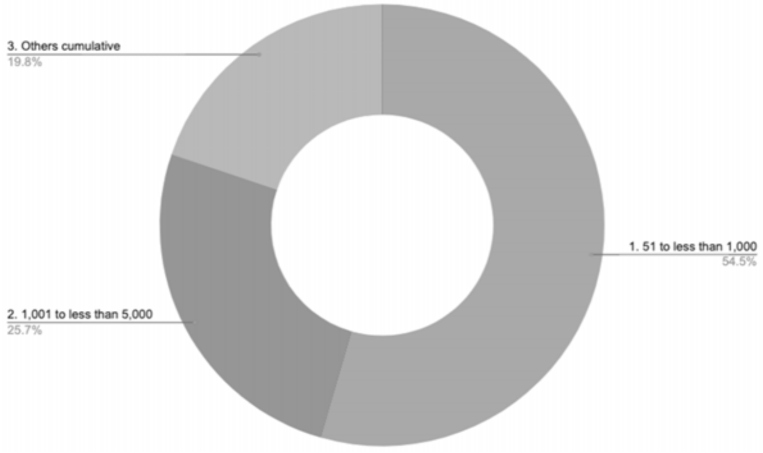

Fig. 4 Overall Organization Size Representation

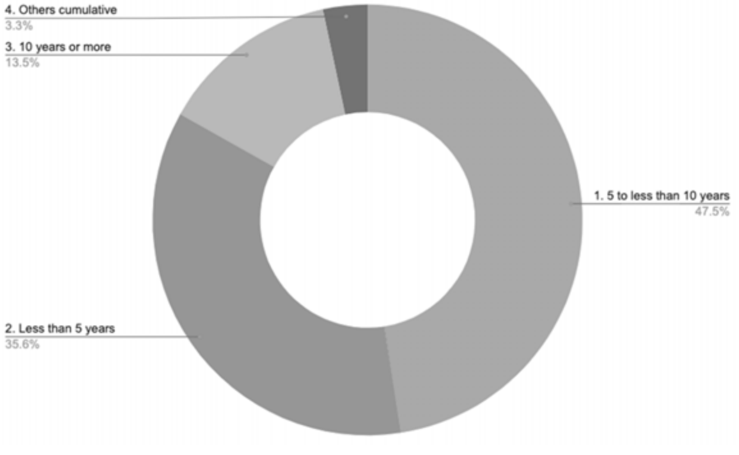

Fig. 5 Overall Experience in IS Representation

Open Science Index, Computer and Information Engineering Vol:16, No:4, 2022 publications.waset.org/10012500.pdf

The job titles of the participants are widely distributed from IS Professionals (29.7%), Managers (22.77%), Software Engineers (11.88%), and Data Engineers (8.91%). Fig. 6 depicts the overall representation of the job titles in the sample. Regarding locations, 44.55% respondents are from the state of New South Wales (NSW), 39.60% from Victoria (VIC), and 11.88% from Queensland (QLD). Fig. 7 depicts the overall representation of the participants states.

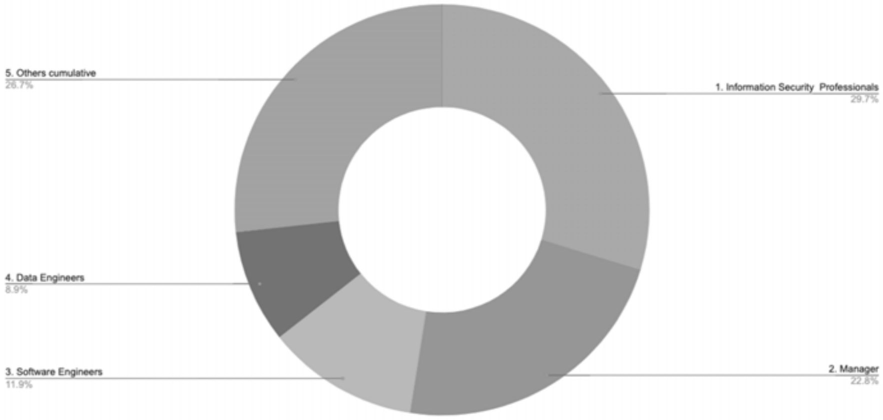

Fig. 6 Overall Job Titles Representation

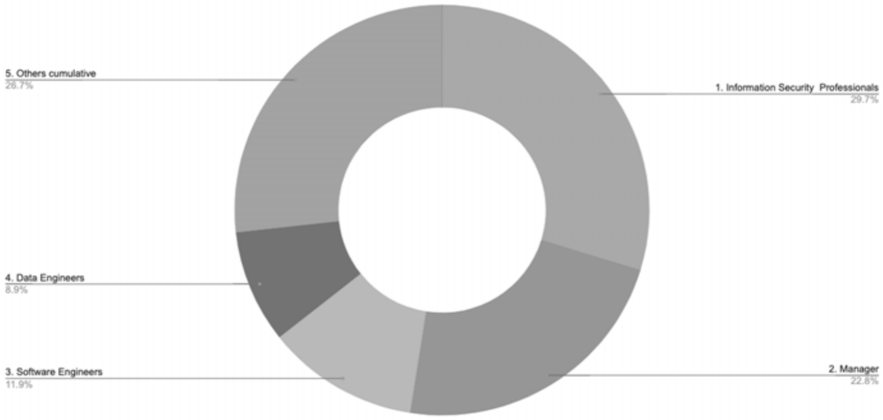

Fig. 7 Overall Location by State Representation

Only 3 out of 104 of the participants skipped the section related to demographics information, which accounts for 2.9%.

B. Hypothesis Testing

For the purpose of this study, the four survey questions with the highest correlation were used for the analysis of the established null hypotheses. Table II presents the specific survey questions subjected to the analysis. Chi-Square was utilized to determine whether two categorical variables are associated with one another within the established population. Using a significance level set at .05, Chi-Square helped observe and test each of the four hypotheses to determine the association of the categorical variables for each hypothesis.

C. Findings

This study was undertaken to provide insights into the governance, risk management, and compliance factors that include cloud computing adoption. The following four research questions drove the study main objectives:

- RQ1: What are the critical governance, risk management, and compliance factors influencing the adoption of cloud computing?

TABLE II
SURVEY QUESTION AND CORRELATION TO HYPOTHESES ANALYSIS

Survey Question	Hypotheses	Correlation Coefficient
Q10: Your organization considers the risks are too high to justify the cost-savings or business benefits of cloud computing.	$H_0$1: There are no critical governance, risk management, and compliance factors influencing the adoption of cloud computing.	.463
Q13: Data privacy and protection legislations outside of Australia limit your organization from adopting cloud computing.	$H_0$2: The concerns of data security and privacy protection do not restrain the management's decision in adopting cloud computing.	.436
Q12: Australian regulatory and compliance requirements negatively impact the decision of your management in adopting cloud computing.	$H_0$3: Regulatory and compliance requirements do not negatively impact the management's decision in adopting cloud computing.	.483
Q14: The NDB scheme of 2017 has a negative impact on your cloud environments.	$H_0$4: The existing laws and regulations are not sufficient to protect the privacy, access, and confidentiality in the cloud environments.	.495

- RQ2: Do the concerns of data security and privacy protection restrain the management's decision in adopting cloud computing?
- RQ3: Do regulatory and compliance requirements negatively affect the management's decision in adopting cloud computing?
- RQ4: Do the existing laws and regulations in Australia protect the privacy, access, and confidentiality in cloud environments?

Hypothesis testing using Chi-Square tests of independence was undertaken to evaluate the research questions. The tests rejected the null hypothesis in all four cases and accepted the alternative hypothesis. Support for the rejected null hypothesis is based on the findings that there are a moderate relationship and strong correlation between the factors identified for this study. The performed analysis indicates that the results are statistically significant (n = 103, $p = .05$). Table III presents the results for the analysis of each proposed hypothesis. The established correlation only suggests the potential degree of influence of the independent variables on the dependent variable [15].

TABLE III
SUMMARY OF HYPOTHESIS RESULTS

Hypothesis	Result
H1: There are the critical governance, risk management, and compliance factors influencing the adoption of cloud computing.	Accepted
$H_0$1: There are no critical governance, risk management, and compliance factors influencing the adoption of cloud computing.	Rejected
H2: The concerns of data security and privacy protection restrain the management's decision in adopting cloud computing.	Accepted
$H_0$2: The concerns of data security and privacy protection do not restrain the management's decision in adopting cloud computing.	Rejected
H3: Regulatory and compliance requirements negatively impact the management's decision in adopting cloud computing.	Accepted
$H_0$3: Regulatory and compliance requirements do not negatively impact the management's decision in adopting cloud computing.	Rejected
H4: The existing laws and regulations in Australia protect the privacy, access, and confidentiality in cloud environments.	Accepted
$H_0$4: The existing laws and regulations in Australia do not protect the privacy, access, and confidentiality in cloud environments.	Rejected

The analysis of the collected data outlined sub-research questions based on the 104 survey participants. The findings include all the questions which the participants agreed and strongly agreed with. Table IV summarizes the findings with their representative categories.

TABLE IV
SUB-QUESTIONS FINDINGS

Area	Finding
Governance	88.46% Agree/Strongly Agree that their organizational IS policies consider cloud computing. 67.31% Agree/Strongly Agree that their organization has a dedicated position in charge of maintaining the confidentiality, availability, and integrity of their cloud computing environments. 54.8% Agree/Strongly Agree that the management of their organization understands and exercises its data governance responsibilities. 78.85% Agree/Strongly Agree that their organization integrates security, privacy, and compliance as part of cloud computing from the initiation of the project.
Risk Management	84.61% Agree/Strongly Agree that security is a primary consideration of their organization when adopting cloud computing. 83.66% Agree/Strongly Agree that their organization prefers to store data in the cloud located within Australia. 77.88% Agree/Strongly Agree that their organization performs a risk assessment as part of cloud computing implementation projects. 66.02% Agree/Strongly Agree that their organization considers the risks are too high to justify the cost-savings or business benefits of cloud computing.
Compliance	71.84% Agree/Strongly Agree that their organization performs regular compliance assessments of the cloud supply chain. 61.16% Agree/Strongly Agree that Australian regulatory and compliance requirements negatively impact the decision of their management in adopting cloud computing. 71.85% Agree/Strongly Agree that data privacy and protection legislations outside of Australia limit their organization from adopting cloud computing. 61.17% Agree/Strongly Agree that the NDB scheme of 2017 has a negative impact on their cloud environments.

The study used a high-level holistic framework that helped outline the areas under consideration. The initial framework was updated to reflect the findings and considerations following the analysis of the collected data. Fig. 8 depicts the relevant findings and their relationship with the area under consideration.

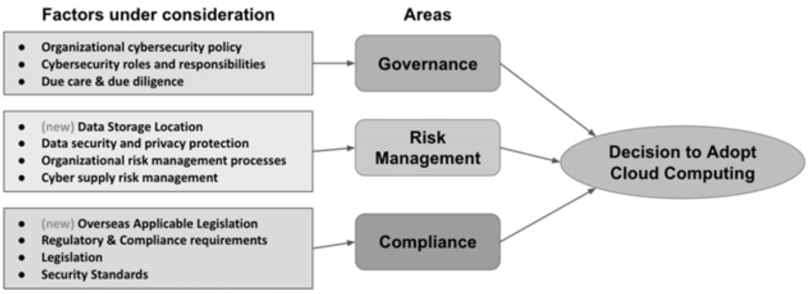
Factors under consideration
Areas
Organizational cybersecurity policy
Cybersecurity roles and responsibilities
Due care & due diligence
Governance
(new) Data Storage Location
Data security and privacy protection
Organizational risk management processes
Cyber supply risk management
Risk Management
Decision to Adopt Cloud Computing
(new) Overseas Applicable Legislation
Regulatory & Compliance requirements
Legislation
Security Standards
Compliance

Fig. 8 Updated Holistic Decision-making Framework

D. Implications for Practitioners and Policy Makers

The study identified the current perceptions of governance, risk management, and compliance expectations that impact cloud computing adoption in Australia after the data privacy and protection changes introduced by the NDB scheme. For IS practitioners, this search provides explicit insights into the expectations for security, data privacy, and compliance for cloud computing projects and their influence on decision-makers' willingness to adopt these types of technology. It is also important to point out that these new findings can apply to existing cloud-based environments. Therefore, this study's knowledge can be utilized during the assessment of IS practitioners' cloud environments and help determine the priorities for mitigation of potentially vulnerable legacy systems that process and store data outside of Australia, which could require additional levels of protection and resources to maintain compliance. By utilizing this knowledge, policymakers can gain critical insights into opportunities to refine and establish more effective and efficient regulatory and policy requirements. Furthermore, the knowledge can support the delivery of the core pillars of the Australia's Cybersecurity strategy which include uplifting the protection of Australian businesses and critical infrastructure. It can help determine requirements for the security of cloud-based products and services by ensuring that sufficient levels of compliance are maintained by their providers. Moreover, the findings can support the development of cloud-specific procurement guidelines to ensure data protection requirements are addressed by the vendors in the supply chain. Considering the study results, policymakers can leverage the Australian industries' expectations to better align future cybersecurity guidelines for cloud environments. These guidelines can establish a baseline for built-in cybersecurity in cloud computing services and harmonize with international standards, allowing for improved security across the whole cloud supply chain. Ultimately, it can help raise the overall cyber-resilience of Australian industries and government agencies.

E. Recommendations for Future Research

Recommended future research builds upon the results and findings in this study by providing an opportunity to IS practitioners to determine the prospective preventative methods, solutions, and policies to mitigate the impact on the significant factors influencing the adoption of cloud computing in Australia, after the regulatory and compliance changes related to data and privacy protection. Future research could build upon the results of this study and include distributing the survey to a more targeted audience such as policymakers and government agencies to determine their attitude related to the topic. This may lead to additional theoretical and practical considerations regarding the formulation, development, and implementation of policies, frameworks, guidelines, and best practices for Australian industries.

V. Conclusion

The process of identifying, evaluating, planning, and fulfilling decision-making duties for adopting new technologies could be a complicated activity for both IS professionals and managers [18], [34], [35]. It is becoming even more complicated to effectively assess the impact on cloud adoption due to the increasing complexity of regulatory and compliance requirements related to data and privacy protection in Australia. The factors differ with the uniqueness of each organization and the industry that it operates. The findings of this study suggest that the relationship between governance, risk management, and compliance areas plays an essential role in adopting cloud computing within Australian organizations. These findings present initial steps towards a further understanding of what drives successful IS for adopting cloud computing in Australia after the NDB scheme took effect in 2018. The extensive literature review, data collection from the research site and the data analysis helped to successfully identify and assess the current areas that impact the adoption of cloud computing in Australia after the recent regulatory changes. The results and findings of this research can contribute to new information and knowledge for future researchers, policymakers, businesses, and IS practitioners in various industries, including information technology, professional services, finance, healthcare, government, academia, and emerging economic sectors in Australia.

References

[1] Deloitte, "Harnessing public cloud opportunities in the government sector," Deloitte, 2019.

[2] "State of the Cloud Report," RightScale, 2019.

[3] McAfee, "Cloud Adoption and Risk Report," 2019.

[4] J. Lu, "Assessing the Cost, Legal Fallout of Capital One Data Breach," 2019.

[5] T. Kajiyama, M. Jennex, and T. Addo, "To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions," *Information & Computer Security*, vol. 25, no. 5, pp. 634–659, 2017.

[6] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, "Cloud computing security issues challenges: A Review," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020, pp. 1–5.

[7] I. Senarathna, W. Yeoh, M. Warren, and S. Salzman, "Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs," *Australasian Journal of Information Systems*, vol. 20, 2016.

[8] S. Tomas, M. Thomas, and T. Oliveira, "Evaluating the impact of virtualization characteristics on SaaS adoption," *Enterprise Information Systems*, vol. 12, no. 3, pp. 259–278, 2018.

[9] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," *Government information Quarterly*, p. 101419, Oct. 2019.

[10] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, Nov. 2016.

[11] C. Yang, Q. Huang, Z. Li, K. Liu, and F. Hu, "Big Data and cloud computing: innovation opportunities and challenges," *International Journal of Digital Earth*, vol. 10, no. 1, pp. 13–53, Jan. 2017.

[12] APRA, "Prudential Standard CPS 234 Information Security," 2019.

[13] P. Leonard, "The new Australian Notifiable Data Breach Scheme," Data Synergies, 2018.

[14] J. W. Creswell, *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Pearson/Merrill Prentice Hall, 2008.

[15] K. F. Punch, *Introduction to Social Research: Quantitative and Qualitative Approaches*. SAGE, 2013.

[16] R. M. Thorndike, "Correlational procedures for research," *Wiley*, 1976.

[17] S. Durst, C. Hinteregger, and M. Zieba, "The linkage between knowledge risk management and organizational performance," *J. Bus. Res.*, vol. 105, pp. 1–10, Dec. 2019.

[18] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Key Dimensions for Cloud Data Governance," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 379–386.

[19] H. Gangwar, "Cloud computing usage and its effect on organizational performance," *Human Systems Management*, vol. 36, no. 1, pp. 13–26, 2017.

[20] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[21] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," *Future Generation Computer Systems*, vol. 57, pp. 24–41, 2016.

[22] K. Brandis, S. Dzombeta, R. Colomo-Palacios, and V. Stantchev, "Governance, Risk, and Compliance in Cloud Scenarios," *NATO Adv. Sci. Inst. Ser. E Appl. Sci.*, vol. 9, no. 2, p. 320, Jan. 2019.

[23] W. Hussain, F. K. Hussain, O. Hussain, R. Bagia, and E. Chang, “Risk-based framework for SLA violation abatement from the cloud service provider’s perspective,” *The Computer Journal*, vol. 61, no. 9, pp. 1306–1322, 2018.

[24] J. W. Creswell and D. J. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications, 2017.

[25] W. M. Trochim, K. Arora, and J. P. Donnelly, *Research Methods: The Essential Knowledge Base*. Cengage Learning, 2015.

[26] A. Fink, *Conducting Research Literature Reviews: From the Internet to Paper*. SAGE Publications, 2019.

[27] S. Islam, S. Fenz, E. Weippl, and H. Mouratidis, “A Risk Management Framework for Cloud Migration Decision Support,” *Journal of Risk and Financial Management*, vol. 10, no. 2, p. 10, 2017.

[28] R. A. Rothrock, J. Kaplan, and F. van Der Oord, “The board’s role in managing cybersecurity risks,” *MIT Sloan Management Review*, vol. 59, no. 2, pp. 12–15, 2018.

[29] M. Burgess, “Protecting data from attackers: Cyber security experts in demand,” *News Limited*, News Limited, 04-Nov-2017.

[30] R. Kumar and R. Goyal, “Assurance of Data Security and Privacy in the Cloud: A Three-Dimensional Perspective,” *Software Quality Professional*, vol. 21, no. 2, pp. 7–26, 2019.

[31] J. Meese, P. Jagasia, and J. Arvanitakis, “Citizen or consumer?: contrasting Australia and Europe’s data protection policies,” *Internet Policy Review*, 2019.

[32] D. Watts and P. Casanovas, “Privacy and Data Protection in Australia: A Critical overview,” 2018.

[33] D. Yimam and E. B. Fernandez, “A survey of compliance issues in cloud computing,” *Journal of Internet Services and Applications*, vol. 7, no. 1, p. 5, May 2016.

[34] A. Furfaro, T. Gallo, A. Garro, D. Saccà, and A. Tundis, “Requirements specification of a cloud service for Cyber Security compliance analysis,” in *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, 2016, pp. 205–212.

[35] E. S. Rubóczki and Z. Rajnai, “Moving towards cloud security,” *Interdisciplinary Description of Complex Systems: INDECS*, vol. 13, no. 1, pp. 9–14, 2015.