International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol.5 Issue 5, May – 2021, Pages: 48-57

An IT Security Framework For Industry-Based Cloud Computing Projects

1Abdool Qaiyum Mohabuth and 2Teshawdeo Mungroo
1Faculty of Information Communication & Digital Technologies, University of Mauritius, Reduit, Mauritius
a.mohabuth@uom.ac.mu
2Ceridian Mauritius Ltd , Cyber Tower 1, Ebene, Mauritius
Vashil.Mungroo@ceridian.com

***Abstract*—** *The movement towards cloud computing platform has gained momentum over the past few years. It has been accepted by the majority of organisations worldwide, since the cloud offers a cost-effective way to manage, control and promote efficiency in project management operations. Customers gain numerous services from the cloud such as wide-ranging network access and on-demand services. The increasing dependency on cloud projects globally makes its use critical and if not properly managed, can affect millions of users at once. Despite the numerous advantages related to cloud computing projects, there are still apprehensions from the part of many organisations as regards to the security issues. Migrating to cloud computing presents issues for example access control and security vulnerabilities in terms of data security. The existing traditional risk management frameworks showed shortcomings towards the increasing complexity of the cloud environment. A survey was carried out targeted towards the IT professionals working in the cloud environment to extract the security issues. From the data gathered, a risk management framework was proposed with enhanced features from existing ones. The proposed framework was then evaluated by security experts at two IT companies where results proved to be quite convincing. This would help project managers to have a safer and more robust way to minimise risks associated with the cloud.*

Keywords— cloud computing, computer security, framework, risk management, access control, vulnerabilities

1. INTRODUCTION

The concept behind cloud computing is to offer a huge number of services while decrease the server spread, wasteful aspects and high organisation [1]. It allows consumers to remotely access the services from a pool of resources that are shared and provided by third party. Cloud computing technology holds three main features:

1. Wide-ranging Network Access: Cloud services should be easily made available through almost all types of electronic mechanisms.

2. Resource Pooling: The cloud services should be fast, efficient and secure enough while handling thousands of data and consumers at the same time remotely.

3. Rapid Elasticity: At any point in time, consumers should have access to their resources and retrieve them as per their demand.

Cloud computing is such a massive success that global organisations adopted it to make the most out of their projects. [2] positively supported the fact that cloud makes project management and storage safe, inexpensive and effective. It is very essential to understand the use of efficient risk management in cloud computing projects to correctly control safety problems and other hazards [3]. In spite of incorporating so many advantages, cloud computing comes with numerous risks that regular users may need to face. Some fundamental safety concerns include data security, consumer information security and distributed computing organisation. Security becomes a major issue. As several organisations such as government agencies and banks upload sensitive data and personal data in the cloud environment. This attract the attention of intruders and in many cases, security has been breached. Data has been stolen and misused which adversely affected corporations and businesses that store sensitive information. Issues like these can trigger fear and lead institutions to reconsider their choice to migrate their data in cloud.

Cloud computing has two distinct features that can be exploited due to the gaps in the existing traditional model: (1) Huge scalable model where cloud computing offers the capacity to scale to countless systems. The cloud architecture dynamically changes according to customer requirements. This feature may prompt traffic flood issues to occur and very often the traditional framework fails to oversee so much information being transferred at once; (2) Multi-Tenancy where cloud computing enables several consumers to make use of the same services. Based on this feature, the personal contents of a customer in the cloud are not controlled by the customer, but by one or more cloud providers. The traditional framework provides insufficient security, as gaining access to one customer's data means that it is not impossible to access another customer's data too.

2. LITERATURE REVIEW

Security risks in cloud computing can be viewed from three different angles namely consumer, service provider and the Government: (1) Consumer viewpoint where failure of cloud computing services may lead to a drop in consumer trust, sensitive and classified data being stolen; (2) Cloud provider who needs to find out the most effective method to guarantee the safety of cloud data, to prevent unauthorised access by hackers; (3) The government where the challenge is to find the most effective method to upgrade the security assurance of a huge scale server data center, how to safely deal with the various size of cloud specialists and how to assess and rank the security levels of cloud providers [4]. Risk framework is described as structures which are essential for developing a risk assessment and vulnerability-reduction cyber security system [5]. Protection of knowledge may use these mechanisms to identify and prioritise the activities required to construct protection into an enterprise. Frameworks can also be customised to solve particular security problems to satisfy the requirements and usage needed. [6] came forward with a proposal to assess the degree of risk that depends on the probability of an occurrence situation, mapped against the evaluated negative effect. It is given by a risk misusing weakness with a given likelihood. The prospect of every single event and the business effect was resolved in an interview with the expert gathering and totalling to this information, portrayal on their combined participation. [7] came forward with an information risk management framework which was intended to offer better comprehension for demanding areas in cloud computing, to analysing risk and recognising weakness. It covers all three cloud services models and also all the deployment models. Cloud suppliers can apply this structure to their organisations to perform risk reduction. Although, it was found to be a good model to identify risks, yet all the findings were qualitative and as a matter of fact, no metrics could be deduced making it difficult to compare without numbers.

[8] proposed a rather new security risk system at that time. It was based on the Software as a Service (SaaS) model with an open deployment model conforming to the standards of the ISO/IEC 27005 standard. The model took into consideration the cloud supplier and the cloud user in the risk evaluation process by ensuring an open connection between them. The goal was to adjust the practical outcomes gained from the involvement of both parties and the potential multifaceted nature which might happen because of their inclusion. In the first phase of the process, each customer should begin its own setting foundation for its data which would move to the cloud platform. Besides, the equivalent was applied to the hazard appraisal process. Only then, the cloud supplier would be able to carry out his risk analysis process. This framework was seen to be functional but only to a certain extent. The process of risk assessment was delayed because the customers need to be informed at each phase that their involvement was needed. [9] came forward with a risk management framework to identify potential issues. It was based on a semi-quantitative approach where the risks identified were given a certain weight. The analytical hierarchy process (AHP) was used to compare each goal based on the weight assigned. The risk factor values would lead to the estimation of the total risk calculation. Each risk factor is evaluated through the result of its probability and effect. The drawback of this model could be noticed by increasing the number of goals in the project. By doing so, the estimation was resulting in being more complex.

Project managers should give appropriate measures to control and avert such dangers and issues [10]. The risks mentioned above will continue to rise unless a more dynamic framework is considered. Past research has helped detect the presence of various security issues in cloud computing, but few have made arrangement on how such risks can be properly handle in a real-life scenario. The idea behind this research is to develop an IT security risk management framework which will solve the aforementioned risks.

3. METHODOLOGY

It was important to seek the perspective and opinions of experts in the field. A questionnaire was used to get a better insight into how organisations deal with security issues on cloud computing. Purposive sampling was used for the purpose of the study in order to select the participants. The questionnaire included likert-scale questions, open-ended questions were also included in order to give the experts freedom to answer specific questions in their own perceptions. The questionnaire consisted of no more than 25 questions and all of them were based on the security aspect of cloud computing. It was structured to use quantitative methods to gather data from IT professionals practicing in IT settings. The questionnaire was divided into distinct parts with specific questions related to security issues in the cloud environment and their strategy used to tackle them. It contained four sections which enveloped (1) Cloud Computing Awareness; (2) Security Risks in cloud computing Projects; (3) Security Features in cloud computing; (4) Demographic Information. The questionnaire was first piloted with twelve security experts who reviewed the survey from the cloud department. The pilot test used a correlation analysis of internal consistency known as the Cronbach Alpha which resulted in the value of 0.87 lying in the excellent reliability-consistency level, as it is greater than 0.80. Details of the 18 likert-scale items are shown in Table 1. Subsequently an enhancement was given the questionnaire before it was made accessible to respondents via the google form. The final questionnaire was then accessed by Cloud IT security professionals, especially technically skilled personnel engaged in the deployment, operation or participation of information security in cloud environments.

Table 1: Reliability Statistics

Items	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Cronbach's Alpha if Item Deleted [a]

User-based Authorisation	21.61	32.65	0.85
User Restrictions	22.09	27.70	0.83
Encryption	22.12	28.34	0.84
Archive	21.59	32.52	0.85
Security Mechanism	21.28	30.18	0.85
Backup Guidelines	21.16	24.80	0.80
Mechanisms	21.01	26.27	0.82
Breakdown Guidelines	20.98	24.78	0.80
Audit Log	21.01	24.59	0.80
Guidelines	21.01	24.97	0.81
Data Integrity	25.71	19.12	0.87
Secure Deletion	25.60	19.91	0.88
Trust	25.41	21.06	0.88
Web Browsing	25.75	20.32	0.88
Denial of Service	25.90	20..98	0.89
Shift	25.75	26.77	0.94
Backup	25.75	20.39	0.88
Monitoring	25.75	20.39	0.88

4. RESULTS & DISCUSSIONS

80 cloud specialists responded to the survey of whom 7.5% were managers, 33.8% cloud specialists, 41.2% cloud security support staff and 17.5% policymakers. Most of the respondents strongly agreed that there exists an existing security policy regarding cloud computing in their organisations. This was confirmed with 57.5% who strongly agreed that the policy was strictly followed. In identifying the security factors, responses relating to confidentiality resulted in strong favour of user-based authorization process (80%), user restrictions (57.8%), and encryption of data (67.5%), which made confidentiality an important factor. Integrity became the second factor after obtaining securing deletion (58%), trusting element (65%), monitoring (68%) and secure archiving (75%). Availability is the third factor after considering ensuring denial of service (68%), shifting to other cloud platform (66%), recovering data from cloud (65%), backup security processes (66%). Reliability is also found to be another important factor after obtaining 67% for mechanisms in place to deal with cloud storage failure, guidelines in place to deal with cloud storage failure (62%), proper monitoring and viability of cloud computing system (65%). In addition to the cloud infrastructure stability, the participants firmly acknowledged that network layer and device control would be among the primary security steps to enhance reliability in the cloud environment. Auditability has also been identified as another important factor in having secure cloud computing system following existence of audit log that keeps track of users accessing cloud data (55%), guidelines in place which document process transparency and traceability of cloud system. (65%). Most respondents strongly agreed that there were audibility checks performed in their organisation to ensure transparency regarding the cloud process. These key factors identified from the survey were used in setting up the framework. The Analysis of Variance (ANOVA) test was used to see if there is any statistical differences between means among participants towards cloud computing and its security challenges due to Gender, Position, Education, and Experience. The parameters considered under each case were based on Standards and protocols, User based authorization , User restrictions, encryption, archives and backup guidelines. P-value was found to be far greater than the level of significance $\alpha = 0.05$ under gender which confirms that this factor did not influence the cloud computing security challenges. However, it was noted that some parameters have p-values < 0.05 when it came to position, education and experience as shown in Table 2. Since p-values for user authorization, restrictions, and backup guidelines are less than the 0.05, then this means there is a significant difference among the respondents regarding position. Similarly, the level of Education and Experience have an impact on securing cloud computing. The framework therefore needs take into account these aspects.

Table 2: ANOVA test

	Gender		**Position**		**Experience**		**Education**	
	F	**Sig**	**F**	**Sig**	**F**	**Sig**	**F**	**Sig**
Standards and protocols	0.64	0.43	1.25	0.30	9.79	0.00	16.33	0.00
User-based authorization	0.08	0.78	3.14	0.03	1.83	0.15	4.13	0.00
restrictions	3.02	0.09	3.58	0.02	7.73	0.00	6.13	0.00
encryption	0.31	0.58	1.89	0.14	10.38	0.00	9.49	0.00

Archive	0.80	0.38	2.22	0.09	1.41	0.25	1.88	0.16
Backup Guidelines	0.00	0.96	6.84	0.00	0.43	0.74	0.73	0.49

4.1 The framework

The framework developed was based on the ISO27005 model as a baseline which was then enhanced to provide a more robust and efficient framework for cloud computing security risk management. The ISO27005 was based on establishing the context, identify risk, assess risk, manage risk, monitor and review risk. Based on these and taking into account the findings from the survey, the following framework was designed and it considered seven phases:

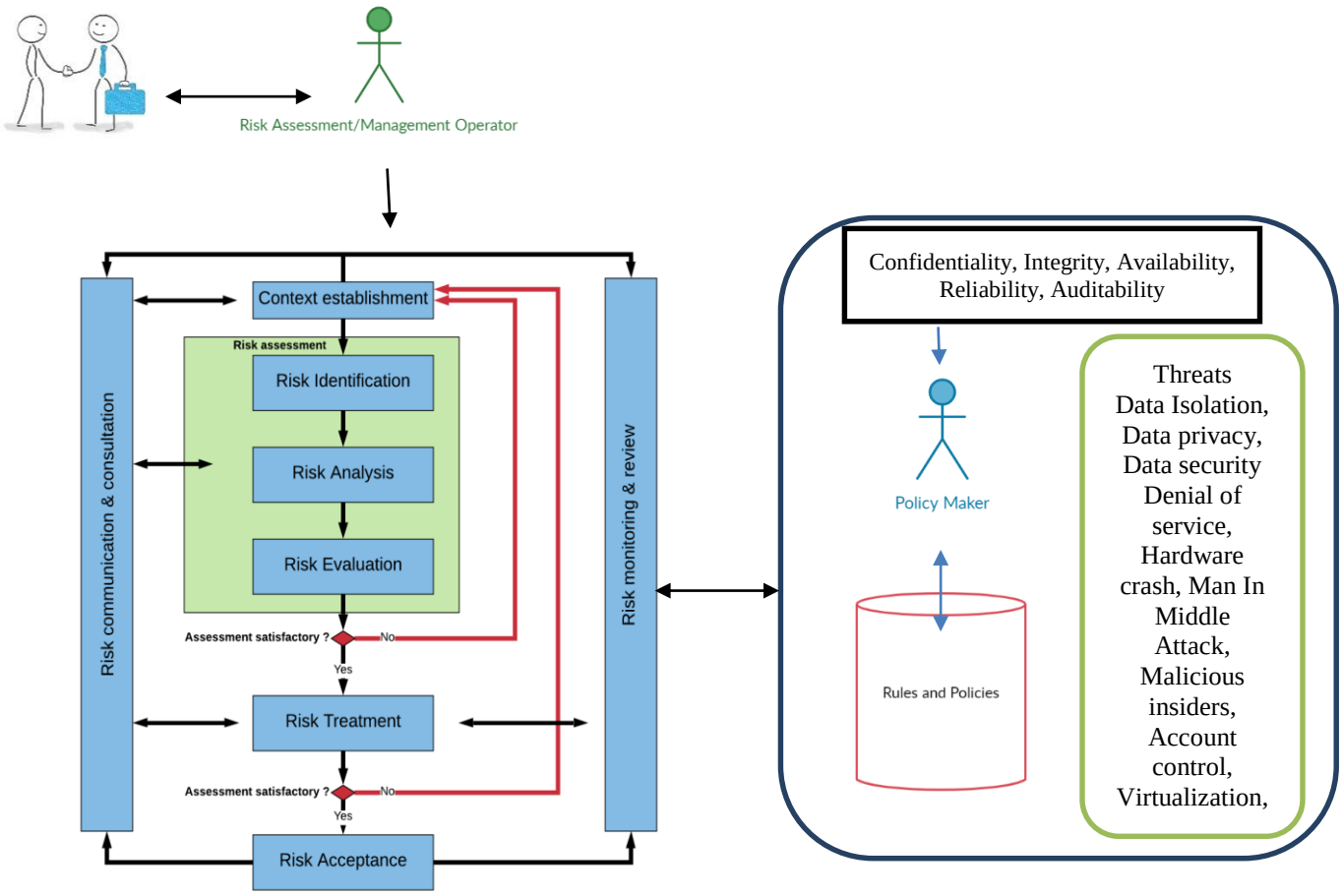

Figure 1 *Proposed cloud computing framework*

The scenario follows as such: A consumer decides to opt for the use of cloud computing instead of storing the data locally. The cloud platform has a cloud service provider typically a third party which specialises in providing cloud storage services. The cloud provider would make use of this enhanced framework by going through each of its stages. The framework made provision for the cloud-based service to go through a Risk Management Operator (RAO) who would start the first phase that is to establish the context. To perceive that risk was hazardous to an organisation, it was imperative to know what kind of organisation it was and what were its processes. This was because while some potential risks might affect most organisations, there would always be certain risks specific to a particular organisation. The framework would go over the following phases (1) Context Establishment Phase with the purpose to

collect the main objectives of the company. The RAO directed all customers to transmit any relevant information through a Cloud Communicator. Each customer (IT Company) who obtained a confirmation from the RAO must then establish an overview of the current business processes and acceptance criteria as per the strategic goals of the IT company, the business processes, and the value of its personal data properties. The objectives gathered by the customer would then be transformed into the Smart model e.g. To increase profitability. The main reason the Smart model was used was that it offered a simple and clear way of understanding what the company goal was to the cloud provider. (2) Risk Assessment normally involved three crucial sub-tasks notably risk recognition/identification, risk analysis, and its evaluation. (2.1) The Risk Recognition/Identification stage helped to cover the identification of resources, threats, existing potential vulnerabilities, and its consequences. [11] argued that there exists no one logical strategy that identified all potential risks that might arise in one go. A study published by Standards Australia (2004) came forward with the use of brainstorming sessions. Agreeing with this statement, [12] came forward with different techniques including interviews, risk checklists, fishbone diagrams, and brainstorming sessions as proven risk assessment methods. For the proposed framework, the Nominal Groups Technique (NGT) was considered. This technique was characterised as an organized strategy as part of the brainstorming process that empowered commitments from experts and encouraged a speedy understanding of the relative significance of security issues and solutions. Group individuals started by composing down their thoughts and perception, at that point to selection, which they perceived is best. Once experts have proposed their lists, everybody presented their final list, and the proposals were at that point examined and prioritised by employing a weight method. In this phase, the experts should examine the data to be transmitted to the cloud platform to assess the validity of the data. Each expert could review the data that has been migrated to the cloud to assess the value of the data and its effect on the priorities of the company and business processes, to analyse the assets as per their criticality, to recognize the risks that may affect the resources and their vulnerabilities and the potential implications. The difference between a normal brainstorming session and NGT was that the latter is a subprocess of brainstorming (structured form). Also, in NGT, only the most knowledgeable and experienced personnel was handpicked to identify potential risks in an organisation. Various studies have concluded that NGT helped to generate better conclusions and estimates compared to traditional methods. The customers along with the experts involvement are imperative in this stage. Besides, the information generated from the customer allowed the cloud provider to establish the specific requirements for risk evaluation which helped to identify the security restrictions of the clients and to assess their obligations.

4.2 Threat Assessment

The cloud provider may, then, carried out its threat assessment. The provider would make use of a risk alert checklist to clients based on their safety guidelines. The cloud provider would be accountable for incorporating identity management issues and is expected to analyse the data gathered from the customer before resuming with risk analysis and risk assessment. Two key elements needed to be identified namely: (1) the security needs of clients in terms of security factors; (2) what according to them would be the impact and the probability if the security factors were not taken into consideration. (2.2) The Risk Analysis also referred to as risk estimation is the technique of calculating the probable risk and impact.

The Delphi Procedure was used as it was commonly known to be a robust approach employed to appraise the likelihood and its outcome of future occasions. This approach made use of expert's groupings by allowing them to come together, share their perceptions. They were encouraged to spontaneously provide approximations and assumptions to an organiser who would then review the data collected and prepare a final report. The experts at each phase have a complete record of what figures other experts have made, but they did not know who made which estimate. Secrecy allowed the specialists to precise their conclusions openly, empowers openness, and prevents conceding mistakes by changing prior estimates. Table 3 features the Delphi procedural approach involved.

Table 3: Risk Analysis

Steps	Description
Select a person to act as a Facilitator/Moderator	The most crucial step discovers an unbiased individual inside the organisation. It is valuable to have somebody recognizable with investigation and information collection.
Distinguish the Experts	The Delphi method depends on a board of specialists. This board may be your venture group, involving the cloud customer, or other specialists from inside the organization or industry, given he has adequate knowledge about the process.
Featured the Problem	The experts must properly define and break down the problem to guarantee that an exact and comprehensive definition is given.
Iterative Questions - Set One	In the first round, common questions in terms of a survey or questionnaire. The moderator/facilitator would then collect and summarize the reactions, expelling any irrelevant material, and seeking out common viewpoints.

Iterative Questions - Set Two	This phase is dependent on the response to the primary questions, the following questions should delve more profound into the subject to clarify specific issues. The results are again collected and summarize, expelling any unimportant fabric and search for the common estimates only.
Agreement reached	At the end of the Delphi cycle, the specialists will have, agree with estimates, if not, more rounds of questions can be performed.

Utilisation of the Delphi Procedure helped to break down the analysis process and recognizing risk estimates. Also, the Delphi Procedure could help to obtain the probability risks happening on future occasions and what effect they might have on the cloud project. (2.3) Risk evaluation which dealt with having a checklist of evaluated threats ranked in relation to the risk assessment standards. Risk assessment made an estimate of the potential threat level in terms of risk severity level. This was done to determine whether the potential threat/risk was low enough to be accepted by the organisation or hazardous enough to be treated. This framework quantified the risk with probability values which range from 0 to 1, with 0 for least severity level with least impact and 1 for highest possible risk severity level with the greatest impact. Upon completion of the risk analysis stage, a checklist of evaluated threats, that were prioritised and agreeing to the hazard assessment criteria, would be delivered. (3) Risk treatment where in this phase there was the establishment of a policy maker who would make use of rules to execute suitable security controls against possible threats. In doing so, this reduced the burden on the cloud service provider and ensured that some skilled in rules and policies were given the task, making the framework more robust and efficient. Table 4 illustrates the counter actions taken.

Table 4: Counter actions

Risks	Solutions
Denial of Service (DoS)	Access control list
Data Breach	Encryption, Digital signatures
Account Hijacking	Two-factor authentication, Identify access management
Insecure API	Penetration Testing

Any unsatisfactory hazard has to be treated, which suggested decreasing the threat likelihood to stay lower than the set bearable limit. A core objective of risk action plan (treatment) was to generate cost viable alternatives to use countermeasures to reduce unsatisfactory risks. Diverse countermeasures choices could be utilised which implied controlling the probability of the chance event or controlling the effect of the results of the hazard happens. (4) Risk acceptance where the cloud provider needed to guarantee that the action plan successfully diminished the threat to a satisfactory mark. The cloud provider mde use of the risk acknowledgment criteria of the customer as well as legitimise risk acknowledgment choices and guarantee that these threats did not influence other security objective. (5) Risk Monitoring where in this phase it was important to assess the viability of any favoured risk countermeasure. We should gauge the chance level lessening after applying a countermeasure strategy. The Delphi method defined above should be utilised to gauge threat level. Monitoring can be set in terms of mathematical values set between 0 and 1; with 0 no reduction and 1 for reduction. (6) Risk communication and consultation phase where the customer and cloud provider would communicate continually. This phase begins when RAO notifies the customer to begin context foundation and ought to proceed until the conclusion of the method. The Cloud provider should share the risk data dangers with the customer. The RAO then submitted the data to client through cloud communicator. This data incorporated a list of current dangers, the treatment or actions plans that need to be done. This data was then submitted to the client. Constant conversation between the cloud provider and customer empowered the cloud provider which increased confidence. (7) Risk monitoring and review where the cloud provider needed to screen and audit the dangers, for example the esteem of resources, dangers, and security susceptibilities. Another task for the cloud provider was to guarantee consistency between threat management and impact acknowledgment criteria. Each stage may take a certain time. In each stage, the client would be able to upgrade the safety necessities and assessed the execution of the security controls enforced by the cloud provider. In addition, the cloud provider would need to survey the action plan as well as find possible threats.

4.3 Framework Evaluation

The evaluation of the framework was carried out at two companies, Ceridian Mauritius Ltd and SD Worx Mauritius Ltd. Both companies set out their cloud computing objectives under the context establishment phase. Under the next stage of risk identification, each company elected three specialists based on Nominal Group Technique (NGT) to collect data on data safety risks linked to cloud computing which would affect the customer's company's goals and objectives. The moderator requests the experts to recognise potential risks such as a company's most noteworthy dangers. Each expert established the risks based on knowledge, experience with relation to organization goals. They would then assign a numbering system from 1 to 3 representing low severity to high severity. The

table below shows the risk identification stage. After aggregating the risks, four most prominent risks were identified which were communicated to the cloud provider as illustrated in table 5.

Table 5: Risk Severity

Ceridian	**Item**	**Risks**	**Level**
	RISK 1	Denial of Service (DoS)	High
	RISK 2	Data Breach	High
	RISK 3	Account Hijacking	High
	RISK 4	Insecure API	Medium
SD Worx	RISK 1	Denial of Service (DoS)	High
	RISK 2	Data Breach	High
	RISK 3	Account Hijacking	Medium
	RISK 4	Compliance and Legal	Medium

Statements concerning the recognised risks was kept in the risk rules and policies which was controlled by the policymaker. The expert team carried out another set of NGT and the data was then stored in the risk rules and policies. They also defined the risk bearable level while finalising a specification of likely risks as shown in the table 6.

Table 6:Identified risks for Ceridian and SD Worx

Factors	**Ceridian**	**SD Worx**	**Agreegate**
Confidentiality	High	Medium	High
Integrity	Medium	Medium	Medium
Availability	Medium	Low	Medium
Auditability	High	Medium	High
Authorization	High	Medium	High
Reliability	High	High	High
Risk Bearable Level	0.30	0.40	-

The Delhi method used for the risk analysis stage with the assignment of probabilities. The probability that each of the four prominent risks identified would happen was assessed under each of the objective set as shown in table 7.

Table 7: Risk Impact matrix for Ceridian

	RISK1->0.6	**RISK2->0.2**	**RISK3->0.5**	**RISK4->0.7**
Obj 1-> 0.5	0.10	0.25	0.20	0.20
Obj 2-> 0.3	0.35	0.20	0.25	0.10
Obj 3-> 0.2	0.2	0.60	0.25	0.15

The risk evaluation was then carried out which allowed the organisations to decide whether the risk was bearable or not. Bearable risk criteria have been defined, approved, and documented by the relevant committee of experts and stakeholders in phase 2. The committee has agreed that the risk level for a bearable risk should not exceed 0.30 for Ceridian and 0.40 for SD Worx. Table 8 shows the risk level for the two organisations.

Table 8: Risk level for Ceridian and SD Worx

Risk	**Level (Ceridian)**	**Level (SD Worx)**
RISK 1	0.35	0.30
RISK 2	0.60	0.45
RISK 3	0.25	0.55
RISK 4	0.20	0.20
Total Risk = 4	1.40	1.50

For Ceridian Ltd, risk 1 has 0.35 and risk 2 is 0.60, while for SD Worx Ltd, risk 2 has 0.45 and risk 3 is 0.55. This means that for Ceridian, Risk 1 and Risk 2 are termed as "unacceptable" and they needed countermeasures to alleviate the threat levels below 0.30. Likewise, for SD Worx, Risk 2 and Risk 3 needed to be treated. This were dealt with in the risk treatment phase which aimed at mitigating the outstanding risks at a level below or equal to the bearable level for the company. Risk countermeasures were acknowledged by the expert team using the brainstorming methods as shown in table 9.

Table 9: Risks counter measures employed by Ceridain and SD Worx

	Risk Mitigated	**Countermeasures used to mitigate risks**
Ceridian	RISK 1	Access control lists (0.20)
	RISK 2	Encryption (0.1)
	RISK 2	Digital signatures (0.7)
SD Worx	RISK 2	Encryption (0.4)
	RISK 2	Digital signatures (0.7)
	RISK 3	Two-factor authentication (0.5)
	RISK 3	Identify access management (0.4)

Risk monitoring was then carried out. The total risk after the counter measures were applied, were then calculated. The outcome is shown in table 10.

Table 10: Risk reduction matrix

		New Risk Level for risk 1	**New Risk Level for risk 2**
Ceridian	Countermeasure1	0.20	0
	Countermeasure2	0	0.15
	Countermeasure3	0	0.20
	Total Risk after counter measure	0.20	0.35
SD Worx	Countermeasure1	0.15	0
	Countermeasure1	0.10	0
	Countermeasure2	NULL	0.25
	Countermeasure3	NULL	0.10
	Total Risk after counter measure	0.25	0.35

The table above has new risk values where Risk 1 = 0.20 for Ceridian Ltd. This concludes that the new corrected level for risk 1 after applying countermeasures is now (0.35-0.2) =0.15. The same logic applied for Risk 2 = 0.35. Applying the counter measure has helped reduce the risk level from 0.60 to 0.25. The aggregate risk level before applying countermeasures was 1.40. The newer value was 0.85. The change in the figures represented a 39.28% risk reduction level for Ceridian Ltd. The same logic applied to Risk 3 = 0.55 for SD Worx. Applying the counter measure helped reduce the risk level from 0.55 to 0.20. The Aggregate Risk level before applying countermeasures was 1.60. The newer value came to 1.00. The change in the figures represented a 37.50% risk reduction level for SD Worx Ltd. The risks which were deemed above the bearable level have now been treated as shown in table 11.

Table 11: Final risks level for Ceridian and SD Worx

	Risk	**Before mitigation**	**After mitigation**
Ceridian	Risk 1	0.35	0.15
	Risk 2	0.60	0.25
	Risk 3	0.25	0.25
	Risk 4	0.20	0.20
	Aggregate	1.40	0.85
SD Worx	Risk 1	0.30	0.30
	Risk 2	0.45	0.20
	Risk 3	0.55	0.20
	Risk 4	0.30	0.30
	Aggregate	1.60	1.00

5. CONCLUSION

Although, many organisations are reaping their benefits by moving from their traditional systems, several major companies are still skeptical about the idea of migrating to cloud platform due to various security issues. Security is a growing concern especially data security in the cloud. Data is meant to be managed by only those who has access. The proposed framework presented a secure identity with provisions for proper management of risks in the cloud by structuring it under seven phases. Guidelines, standards and best practices were made available, and a specific entity named "policy maker" was added to handle these rules. The framework was tested with real data at two IT companies as detailed above and the result obtained proved to be convincing. Constant communication with cloud clients is very essential for this framework to be effective. It is a proven concept that having clients at the start of the framework process as well as during phases will no doubt improve risk management process. The framework would be of help for convincing companies who still have apprehensions about security issues to migrate safely to cloud computing platform.

6. REFERENCES

[1] Inbarani, S. W., Moorthy, S., G., & Paul, C. K. (2013). An Approach for Storage Security in Cloud Computing - A Survey, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 2, No. 1, 2013, pp. 174-179.

[2] Qin, Z., Xiong, H., Wu, S., & Batamuliza, J. (2016). A survey of proxy re-encryption for secure data sharing in cloud computing. IEEE Transactions on Services Computing.

[3] Youssef, A. E. (2020). A framework for cloud security risk management based on the business objectives of organizations, International Journal of Advanced Computer Science and Applications, Vol. 10, No. 12, 2019, pp. 186-194

[4] Chen, H. (2013). An Information Security Risk Assessment Framework for Cloud Computing. In Advanced Materials Research,Vol. 756, pp. 1469-1473, Trans Tech Publications Ltd.

[5] Amini, A., & Jamil, N. (2018). A comprehensive review of existing risk assessment models in cloud computing, Journal of Physics: Conference Series, Vol. 1018, No. 1, p. 012004, IOP Publishing.

[6] Catteddu, D. (2009, December). Cloud Computing: benefits, risks and recommendations for information security, Iberic Web Application Security Conference, pp. 17-17, Springer, Berlin, Heidelberg.

[7] Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments, 10th IEEE international conference on computer and information technology, pp. 1328-1334.

[8] Gritzalis, D., Stergiopoulos, G., Vasilellis, E., & Anagnostopoulou, A. (2021). Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud, Advances in Core Computer Science-Based Technologies, pp. 109-128, Springer, Cham.

[9] Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A risk management framework for cloud migration decision support, Journal of Risk and Financial Management, Vol. 10, No. 2, 10.

[10] Joshi, C., Singh, U. K., & Kanellopoulos, D. (2018). An enhanced framework for identification and risks assessment of zero-day vulnerabilities, International Journal of Applied Engineering Research, Vol. 13, No. 12, pp. 10861-10870.

[11] Berg, H. P. (2010). Risk management: procedures, methods and experiences, Reliability: Theory & Applications, Vol. 5, No. 2.

[12] von Solms, R., & Willett, M. (2017). Cloud computing assurance–a review of literature guidance. *Information & Computer Security*.

Author's picture should be in grayscale.

Picture size should be absolute 3.18cm in height and absolute 2.65cm in width

Authors

Abdool Qaiyum Mohabuth

Faculty of Information Communication & Digital Technologies,
University of Mauritius, Reduit, Mauritius
a.mohabuth@uom.ac.mu

Teshawdeo Mungroo
Ceridian Mauritius Ltd
Cyber Tower 1, Ebene, Mauritius
Vashil.Mungroo@ceridian.com