CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework

Sugandh Bhatia[1], Jyoteesh Malhotra[2]
[1]Computer Science, Punjab School of Economics, Guru Nanak Dev University, Amritsar-143005, India
[2]Department of Electronics and Comm. Engg., GNDU Regional Campus, Jalandhar-144009, India

Article Info

Article history:

Received Nov 30, 2017
Revised Jun 29, 2018
Accepted Feb 5, 2018

Keyword:

Cloud computing services
Compliance
Privacy
Readiness
Security
Threats

ABSTRACT

The privacy, handling, management and security of information in a cloud environment are complex and tedious tasks to achieve. With minimum investment and reduced cost of operations an organization can avail and apply the benefits of cloud computing into its business. This computing paradigm is based upon a pay as per your usage model. Moreover, security, privacy, compliance, risk management and service level agreement are critical issues in cloud computing environment. In fact, there is dire need of a model which can tackle and handle all the security and privacy issues. Therefore, we suggest a CSPCR model for evaluating the preparation of an organization to handle or to counter the threats, hazards in cloud computing environment. CSPCR discusses rules and regulations which are considered as pre-requisites in migrating or shifting to cloud computing services.

Corresponding Author:

Sugandh Bhatia,
Computer Science,
Punjab School of Economics,
Guru Nanak Dev University,
Amritsar-143005, India.
Email: sugandhcs.rsh@gndu.ac.in

1. INTRODUCTION

The cloud computing model describes a turnaround in the field of Computing and Information Technology. Nowadays, computing is considered as a service instead of computing as a product. It is economically feasible for the companies to avail and obtain the services or resources of information technology, due to cloud computing. Moreover, the domain or area of cloud services is vast and broad. However, the biggest obstacle which is experienced by the companies on the cloud computing platform is the lack of security mechanism. Cloud computing is the latest technology or a new computing paradigm. It includes various issues like security, privacy, risk assessment, compliance and service level agreement. The architecture [1] and structure of the cloud computing is based upon multi tenancy and multi-layer design based model, which produces much convoluted and arduous hazards. Therefore, it is need of the hour that companies, organizations and institutions should adopt an impressive, effective and comprehensive method for cloud computing [2] services to make sure security, safety and privacy of the system. Without taking the support of information technology, it is not possible for any Nation to achieve sustainable growth. In today environment, recent paradigms like Cloud Computing, Big Data, Mobile Networks, Internet of Things [3] and Cloud of Things has enhanced that significance by increasing access to technology that ultimately drives economic growth of a country. The present paper is based upon a report which was released in 2016 by BSA [4]. The Software Alliance with registered office in Washington D.C. On the basis of report, a scorecard has been prepared which ranks the IT infrastructure and policy environment. Major 24 countries are included that account 4/5 of the IT markets globally. Cloud computing readiness should be improved and a policy framework is required to enhance the area or domain of cloud computing services. Developing countries like India, Indonesia, Argentina, Brazil and South Africa can achieve sustainable economic growth and productivity with this computing paradigm. The major findings of the report reveals that cloud capabilities can be deployed to provide optimized, secured, trusted facilities and services. However, due to dearth of standardization of services, secure SLAs and security in the cloud, organizations and companies willing to shift their data or information to the cloud are dubious to perform so. Proper feasibility study is to be accomplished.

Major BSA cloud policy blueprints are:

a. Ensuring Privacy
b. Promoting Security
c. Battling Cybercrime
d. Protecting Intellectual Property
e. Ensuring Data Portability
f. CSPCR readiness to tackle threats of cloud computing.

2. MOTIVATION AND NEED FOR AN ORGANIZATION

Cloud computing delivers attainable supply of services and resources as per requirement that can be controlled comfortably. However, the zippy growth of cloud computing services point out major issues about the pitfalls and hazards affecting cloud security and privacy. The cloud service model [5] is a multilayer model and architecture is based upon multi tenancy which induces fresh and complicated threats and these can be scourging for the cloud systems, service providers, end users and administrators. Hence, it is required that appropriate provisions should be made while designing, developing, deploying and organizing secure and safe resources or services of cloud computing. Before migrating to cloud platform, organizations should verify information and data privacy [6], security and revamp system amenability. The executives of IT firms believe that lack of information privacy and security readiness is one of the major reasons for the hesitation of organizations from transforming to the cloud. Therefore, this paper suggests a model for cloud security, privacy and compliance readiness (CSPCR) for cloud computing services. The objective of this model is to assess the four major cloud organization components –i.e. manpower, information, software or technology and hardware. Technical manpower is responsible for smooth functioning and maintenance of cloud services. Information is received in the cloud environment after the processing of data. Software and technology is the collection of routines, applications and platforms that execute the desired services. Hardware is the collection of peripheral devices networking equipment used in the cloud environment. All these components must be organized, managed, controlled, documented and prioritized. Moreover, the cloud services can’t be commissioned and streamlined without the clearly defined objectives that behave like a back-bone of the organization. The proposed compliance framework is a model created to achieve the objectives and aims of the organization in the CSPCR requirements. The suggested cloud specific CSPCR readiness model analyzed the present condition, CSPCR settings and aspirations of an organization regarding ameliorated security mechanism to secure data on cloud. The model can be used to evaluate manpower, -i.e. network administrators, technicians, software engineers, IT managers and other non-technical personnel. It furnishes suggestions to deploy CSPCR implementations in order to improve the standard of readiness through the adoption of felicitous protection and securing standards.

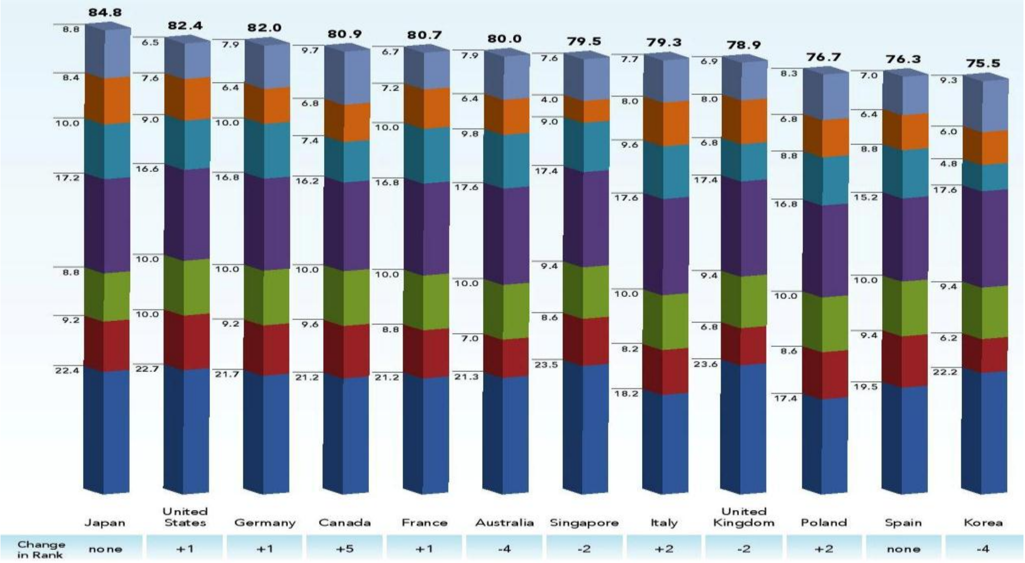

Figure 1. 2016 BSA global cloud computing scorecard (top 12 countries)

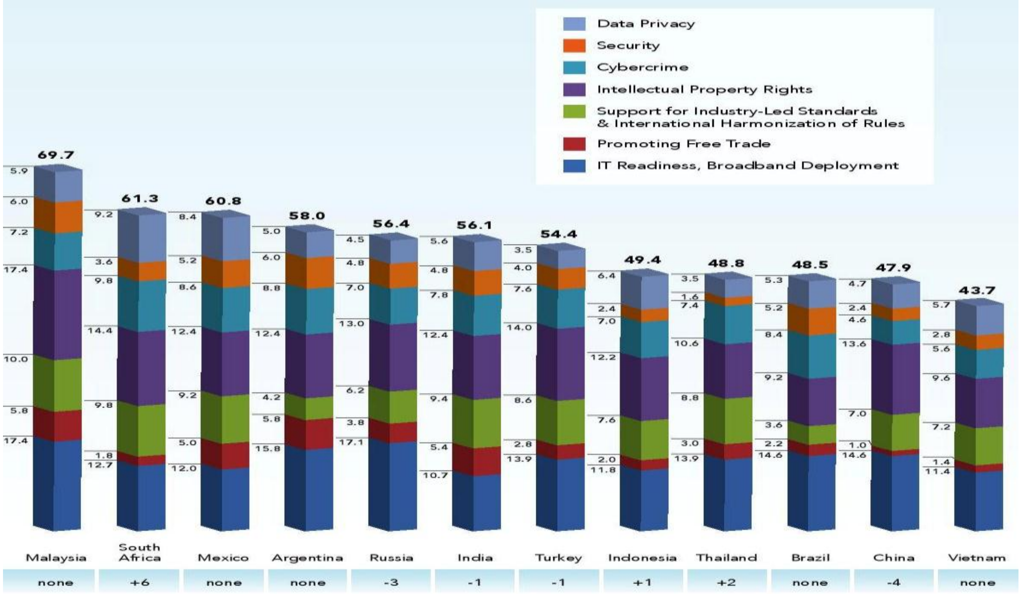

Figure 2. 2016 BSA global cloud computing scorecard (last 12 countries)

3. KEY FINDINGS

The 2016 BSA global cloud computing scorecard divulged important changes in the security and privacy policy of cloud computing in the global economies. The findings are dependent upon a special study and ranking of the 24 major countries (Figure 1 and Figure 2) that account for more than 80% of global IT market. The requirement of privacy and security has produced many favorable results in most of the countries. Law reforms, encryption mechanism and public awareness perform significant role in this. In some countries, Governments have proffered constraints on the cross border exchange of data. If, it is implemented or applied, it will be negative for cloud computing industry. Since 2013, most countries have frameworks for data protection [7] and have appointed autonomous privacy commissioners. Protection laws are based on the organization for economic co-operation, European Union Data Protection Directive and Asia-Pacific Economic Co-operation Privacy principles. However, some countries have applied compulsory registrations for data controllers and cross border data transfers. Whereas, some countries have adopted or proposed prescriptive data localization regimes that would require cloud providers to restrict the free flow of data and

build costly, unnecessary servers in order to provide services in a specific market. The study reveals the availability of infrastructure in each country which is required to support digital economy, cloud computing and its services. National broadband plan, connectivity score of a country and internet bandwidth are three important factors in the comparative statement. Infrastructure score of every country has improved over a period of time. The major improvers are France, Russia, South Africa, Thailand and United Kingdom. Broadband penetration is inconsistent in many countries, but countries like Japan, South Korea and Singapore has implemented National Broadband Networks. The basis of the BSA cloud computing study is legal and regulatory framework of 24 countries which consist 66 questions that directly associated with the readiness of cloud computing. The objective of the study is to suggest a framework which can create an interface between policy makers and providers of cloud offerings with an objective towards creating global conjoin governance of laws and regulations associated with cloud computing. The proposed CSPCR model is designed to assist cloud companies and organizations in transforming to the cloud to manage information security, privacy and compliance readiness.
This model dispenses the following:

a. Dissemination of techniques and methods among the technical personnel in the organization.
b. Evaluation of the readiness of an organization for cloud hazards, threats and compliance risks.
c. Validation and update of information in the organization which ensures impressive utilization, distribution and delivery.

4. RELATED WORK

Cloud computing is one of the most transformative technology in the world. Gartner [8] forecasts that the world wide public cloud services market is estimated to grow by 18 percent in 2017-18 to $ 247 billion, up from $ 209 billion in 2016-17. It is predicted that highest growth will be achieved by infrastructure as a service, which is projected to grow more than 36 percent in 2017-18. Many Government and private organizations are shifting to cloud computing environments. Efficient and successful implementation of cloud services is a complicated task. The outcome of cloud services of most of the organizations is difficult to ascertain. Therefore, advantages and limitations are necessary to understand before considering the readiness to shift to a cloud service model.

According to Sybia *et al.* [9] organizations must have a forensic readiness model which should be based upon cloud performance and capacity. This model assists the cloud service providers to organize and supply the data required for cloud forensic investigations. These cloud forensic investigations are one of the significant ingredients of the cloud information security process and security mechanism functions. However, the proposed model is only capable to analyze the readiness of the cloud data in the system for forensic analysis.

Kao *et al.* [10] suggested a framework for the life cycle of cloud services. The autonomous framework can be applied in any kind of cloud systems. This proposed system handles the risks and threats in the cloud that must be scrutinized, investigated and controlled for compliance and compliance issues with statutory and authoritative requirements. The authors do not furnished a comprehensive method to the cloud security system development life cycle. However, no methodology, phases or models are discussed for executing a cloud based information security system.

Reith *et al.* [11] develop a nine phase digital forensic process model. The phases are identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning of evidence. In this model, first five phases deal with the process of organizing, handling and managing of records. On the other hand, the last four phases in the proposed model perform the job of evaluation, investigation, examination and presentation.

Ben Martini *et al.* [12] presented a coherent digital forensic model to organize, manage and restore digital records and evidences for digital forensic purpose with in the cloud computing environment. This proposed model is based upon two very popular and useful models – McKemmish [13] and NIST (Kent *et al.*) [14]. Authors re-explored these two models to find out the variation to perform digital forensic in cloud computing and digital system environment. The emphasis is on the understanding of technical aspects and consequences of digital and cloud forensics in the cloud computing environment.

Hong *et al.* [15] have presented a new triage model as per the requirements of quick collection of digital evidences by law enforcement personnel who are responsible for the analysis and collection of electronic evidence. Moreover, there are various digital forensic [16] triage tools which are executed to seize crime related information.

5. CLOUD SECURITY, PRIVACY AND COMPLIANCE READINESS MODEL

The suggested CSPCR readiness model furnishes an explication of cloud resources in order to consider the most suitable measure for information security, privacy and compliance in cloud environments. The objective of enforcing cloud based CSPCR control is to presciently ascertain, diagnose, control and to organize the cloud hazards, threats and risks. Controls can also be used to surveil cloud users, their responsibilities, to descry and preclude crisis along with breach of compliance in the cloud environment. The model gives instructions for the analysis of readiness [17] of organization to attain these goals. It defines the phases those should be prosecuted during the life cycle of CSPCR. The cloud CSPCR readiness model constituents propounded in the following segments cover resource manager, IT professionals and system analyst decision making capabilities and cloud data analysis. It is possible for cloud organizations to govern a reliable, precise and amenable readiness assessment. The outcomes can be helpful to analyze that the readiness level is acceptable and satisfactory.

To achieve perspicuity, an organization must gather data apposite to information privacy, security and as per needs of compliance for the:

a. Effective implementation of the migration plan to the cloud.
b. Easy to understand the activities of IaaS, PaaS and SaaS service models of cloud.
c. Efficiently manage, secure and organize cloud assets.
d. Understanding of the present data privacy, security and compliance program which include documentation planning, incident control and response, recovery strategies and software solutions.

To exercise cloud data analytics, an organization must design reports, events and logs to:

a. Simple understanding of threats and risks available in the system.
b. Find out, investigate and remove anomalies from the system.
c. Analyze cloud performance and behavior. In case of peculiar behavior, a solution must be suggested by the experts.
d. Arrange perfect diagnosis to consider condign responses to hazards.

To take right decision, organization must perform the following operations

a. Implementation of appropriate security measures based on the calculated risk controls.
b. Risk measurement and control policies must be reviewed and raised as per requirements.
c. Risk/ threat control and response plans must be initiated and executed for the benefit of organization.
d. Compliance and performance should be evaluated and monitored on daily basis and reports must be given to the management at the earliest.

The suggested CSPCR model is designed to assist cloud organization and those considering shift to the cloud. Requirement of information security, privacy and calculation of compliance readiness can be performed with the help of CSPCR model. This model performs the following:

a. Distribution of data and information among various departments in the organization.
b. Analysis of current data information security, privacy and readiness policies and requirements.
c. Revamping and documentation of cloud information for the purpose of facile implementation and access.
d. Evaluation of the preparedness for cloud hazards, risks, threats and compliance uncertainties.
e. Assessment of technical and professional skills and knowledge of technical personnel in the organization.

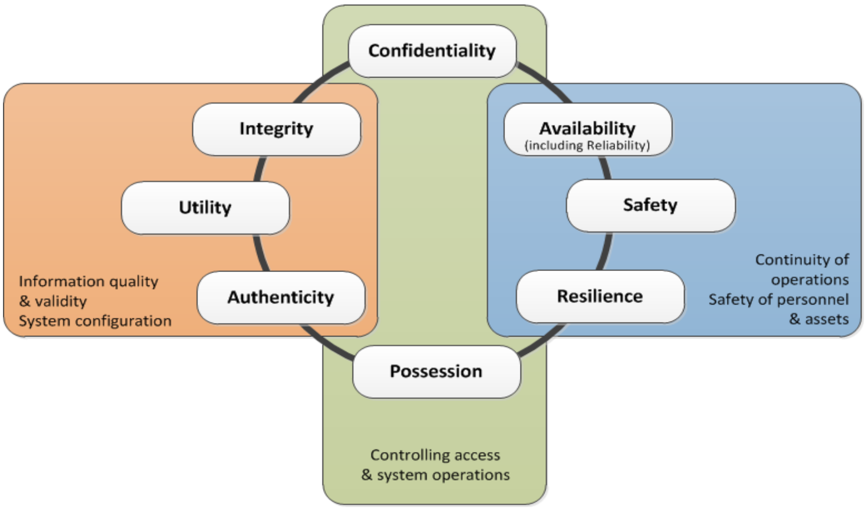

Figure 3. Cloud security, privacy and compliance readiness (CSPCR) hexagonal model

6. CLOUD SECURITY MODEL (A HEXAGONAL MODEL)

A hexagonal model is proposed for cloud security to help cloud service providers and clients in planning to shift to the cloud. It is an associative tool between security plans, policies, control, arrangement and security attributes. All domains or areas of cloud must be taken in to consideration while designing, developing and implementing the CSPCR readiness framework [18]. Figure 3 shows the hexagonal cloud security model. The hexagonal information security model is based upon six basic and two additional attributes. These are resilience, availability, authenticity, confidentiality, utility, possession, integrity and safety. The hexagonal cloud information security model assist cloud companies to make an assessment of risks based on the possibility of hazards and threats occurring in the system. The security model is designed using the Parkerian Hexad [19] proposed by Donn B. Parker in 1998. The Parkerian Hexad is a collection of six elements of information security. There are three additional attributes added by Parkerian Hexad to the classic security attributes of the CIA triad [20] (confidentiality, integrity and availability). Once the areas of CSPCR model is decided, the next phase is to point out and cogitate all those components which perform a pivotal role in information privacy, security and compliance rendition in the cloud system. The most important components are obtained from four classical subsystems of cloud, namely personnel, tools and technology, data or information and hardware. All these factors can be analyzed by the users from various sectors and departments of the organization. The actual measurement of readiness factors is a critical process. The significant factors affecting the readiness of CSPCR model are:

a. Clarity Regarding Objectives and Vision of Organization: Organizations must be aware, sensitive and reactive to security and privacy of information rather than prescient. Security experts proclaim that defined goals are required for applying and implementing the security program effectively and efficiently. Mckay [21] clearly suggested that, it is not possible to achieve and enforce compliance policies, information privacy and security, if the objectives are not defined clearly.
b. Authentication: An organization must apply impressive authentication methods in order to restrict unauthorized access [22] of information on the cloud. Two factors authentication can be applied for this purpose. Moreover, role based access control mechanism can be implemented which is an important method to restraint the availability of information needed to perform a certain task. In today’s business environment, authentication must be implemented at various levels in the system.
c. Control Unauthorized Modification: It is the prerogative of the organization to implement measures to control the unauthorized modification. The integrity of critical and important assets must be maintained by the organization. There must be a mechanism in the system which should control unauthorized alterations and modifications. If these modifications performed in the system, it must be rollback without any delay.
d. Interruption Free Access: Cloud assets and resources must be designed and organized in such a way that various attacks such as denial of service [23] that revoke access of data should be controlled. The flow of information must be without any interruption. Clients are allowed to fetch data any time without any hindrance as per their requirements. Moreover, in case of large amount of data, any data control or management mechanism can be implemented in the system.
e. Training of Personnel: Cloud system must be dynamic and flexible. There should be possibility to modify or alter as per the requirement or demand of the user. Seminars, workshops and conferences must be organized for the training and education of personnel on regular basis after a certain period. This education and training programs perform significant role in achieving information privacy and security in cloud. After the workshop or seminar, skills of the technical personnel must be tested
f. Security Experts in Management: In the top level management of organization, there must be one or two security experts. Most of the times, it has been seen that there are non-technical persons in the management. Only the security expert can understand the importance of privacy and security of information. On the recommendations of technical committee, management can adopt a policy framework for security and this will create readiness in the system for the enforcement of policy in cloud information security and privacy.
g. Security, Privacy and Compliance Policy: The policy reveals the important resources and assets with much detail and explanation of what is favorable or not favorable to ensure privacy, security and compliance. It is a pivot element to impressive cloud security management. The development of a cloud security policy along with readiness framework is an important step in determining the required arrangements for security and privacy.
h. Integrity: It is a mechanism which assures the consistency and accuracy of data available in the system during its life. An autonomous service must be used in the system to maintain integrity on the data and information available on the cloud. Byzantine failures [24] must be controlled with the help of Byzantine fault tolerant service in the system.

7. READINESS ANALYSIS

After the determination of important readiness factors, the next step is to find out the required set up for each factor. The training of technical personnel must be up to that level which can be applied and implemented to achieve and organize security and privacy of information along with compliance controls. The results of readiness analysis are:

a. The present scenario of privacy, security model, compliance management and needs are disclosed.
b. The required framework of cloud information privacy and security will be revealed after the readiness analysis.
c. Compliance and compliance issues can be unmasked which will strengthen policy enforcement and proper planning. It is require to highlighting those areas which may affect security and privacy in the cloud.

When the desired security services has deployed by the cloud organization and has accomplished the required degree of readiness [25], then the most important function is to watch the system to conserve that level of security and readiness. Table 1 gives the example of cloud information privacy, security and compliance readiness level. Six levels are provided for the objective of evaluating the readiness of parameters. Feedback and remarks regarding the levels must be incorporated to reveal the clear situation and a perfect assessment of readiness.

8. FEASIBILITY STUDY

To ruminate if cloud services for the facilitation of CSPCR model are propitious in terms of finance, working, capability, security, maintenance and adaptability, a feasibility study is commingled in the CSPCR readiness model. The feasibility study is implemented after the assessment and analysis of current CSPCR services. The feasibility study consists of two main phases:

a. Economic Feasibility: This type of feasibility includes financial issues and policies related to business and migration. The organization should:
   1) The cost of CSPCR migration and other overheads should be in control and economically feasible.
   2) The privacy, security of information and compliance policy should not be affected with the migration.
   3) The documentation of CSPCR should reflect modifications such as service level agreements and policy implications in support of CSPCR performance and availability.
b. Technical Feasibility: This type of feasibility includes the technical needs to fulfill the demands of CSPCR readiness. The organization should:
   1) Congeniality should be between CSPCR components while shifting to cloud services.
   2) CSPCR issues must be solved and handled carefully by the selected cloud technology. All the resources of the CSPCR must be transferred to the cloud.
   3) Desired goals and objectives of CSPCR must be handled and achieved by selected cloud technology.
   4) Provisions should be made to manage legacy systems [26] and other incompatible traditional systems which are not supported by cloud.

The feasibility study primarily performed with the help of analysts and experts to provide guidelines and decisions of migration to the cloud along with desired modifications to CSPCR system. The economic feasibility is conducted by chartered accountants, company secretaries, cost and work accountants and experts in the field of finance, commerce, economics, statistics and econometrics. Technical feasibility is conducted by system manager, analyst and tester. Various methods or techniques like questionnaires, interviews, surveys and feedback can be used to collect information for performing analysis.

Table 1. Measurement Levels for Cloud CSPCR Readiness

Phase #	Description / Working	Readiness Level	Current Phase	Target Phase	Reviews
1	No information security manual or document is prepared by the organization. Lack of awareness, security and privacy policies and compliance needs. Moreover, due to scarcity of economic and technical resources, it is not possible for the organization to avail all these services.	Not Ready			

2	All the documents regarding the information privacy, security, compliance readiness are available with the organization. The organization is sensitive enough to cyber hazards, attacks, risks and not interested to share and update policy literature and documents. Dearth of training and skill development workshops. Information security, privacy methods and compliance readiness models are ineffectual.	Vigilant			
Phase #	Description / Working	Readiness Level	Current Phase	Target Phase	Reviews
3	The cloud information privacy, security and compliance documents are to the point, understandable and clear. Some documents, methods and functions are disseminated and updated. Trainings and skill development workshops are there, but not regular. Privacy, security and compliance findings fulfill only legal needs.	Partial Readiness	✓		
4	All the documents regarding the information privacy, security, compliance readiness are clear and up to the mark. Most of the documents are updated and disseminated among appropriate personnel in the organization. Training and skill development workshops are organized after regular intervals. Privacy, security and compliance readiness model is effectively implemented and adopted in the organization.	Primary Readiness			
5	The organization has updated, precise and comprehensible information privacy, security and compliance policies. Role and duties of technical personnel must be clear and well defined. All the documents are easily approachable, regularly updated and appropriately disseminated. Training and workshops are organized on priority basis. Seminars, workshop and skill development programs must be the part of organization. Privacy, security and compliance readiness model is executed in an efficient manner with recommended update	Complete Readiness		✓	

9. EVALUATING THE READINESS OF THE SYSTEM

Two important factors in the transformation of the cloud system are readiness analysis and feasibility study. Before the migration, goals of the organizations should be framed out and fulfilled. It is required to sort out all the issues regarding the compatibility, integrity, availability and confidentiality to ensure the successful deployment of the information system to a cloud service provider. Moreover, all CSPCR requirements have been discussed should be in order prior to the implementation of the migration plan. Finally, the migration plan should be reviewed by the team of experts to ensure the proper working of the system at various levels.

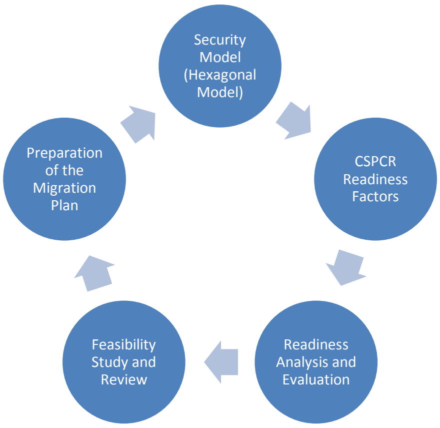
Security Model (Hexagonal Model)
CSPCR Readiness Factors
Readiness Analysis and Evaluation
Feasibility Study and Review
Preparation of the Migration Plan

Figure 4. Constituents of CSPCR compliance readiness model

10. OBJECTIVES OF CSPCR READINESS MODEL

The primary objective of the proposed CSPCR model (Figure 4) is to assist organizations in analyzing their present cloud security, privacy and compliance readiness against hazards and threats of cloud. Many techniques are given by the above said readiness model to help organizations to self-evaluation. Proper assessment of desired readiness level and sustainable growth and implementation of cloud is achieved by CSPCR model. It supports in proper planning and decision making at various levels in the organization to find out new security issues, threats and hazards during the implementation and migration to the cloud. An organization can avail the services of experts to analyze and evaluate the readiness. Both internal and external experts can be used for this purpose. It is recommended to avail the services of internal experts in the system as it ensures the maximum security, privacy and economically favorable for the organization. Only a trusted third party should be assigned to perform the CSPCR assessment with in the stipulated readiness model. The Indian Contract Act, 1872 and Copyright Act [27] (amendment) 2012, confidentiality and non-disclosure agreements should be signed to protect copyright and intellectual property [28] from risks such as sharing, hacking and theft of plans and results of the proposed readiness model.

11. CONCLUSION

Nowadays, Government, private and non-government organizations are thinking to shift or has migrated to the cloud services due to myriad benefits of cloud computing services. As a result, cloud security, privacy and compliance readiness and control have mutated as a prominent research area in the field of computing and information science. The present paper suggests a cloud security, privacy and compliance readiness model that performs a significant role to achieve the upgraded level of security. This readiness model is multi-dimensional and multi layered. It includes a hexagonal security model for analyzing the various domains of cloud information security, privacy and compliance readiness requirements. The CSPCR model can be used to evaluate existing information security, privacy and compliance readiness. The proposed framework determines the organization attitude regarding the managing, controlling, operating, availability, compliant and secure cloud computing services. Moreover, the performance and ability of the technical personnel in the organization can be checked. According to this framework, a special concentration is devoted on organizing workshops, seminars and other activities to uplift the skills, education and awareness in the technical personnel of the organization. The CSPCR model is not designed only for the organizations planning migrate to cloud, but can also be executed to make any improvement in the system. The model can also be used as an optimization tool for the organizations that have implemented the cloud services and creates hazard aware and control environment which applauds prescient and sagacious operations in the system. Hence, this model helps an organization to evaluate any cloud services issues like security, privacy, compliance readiness and compatibility.

Figure 5 shows the CSPCR readiness model.

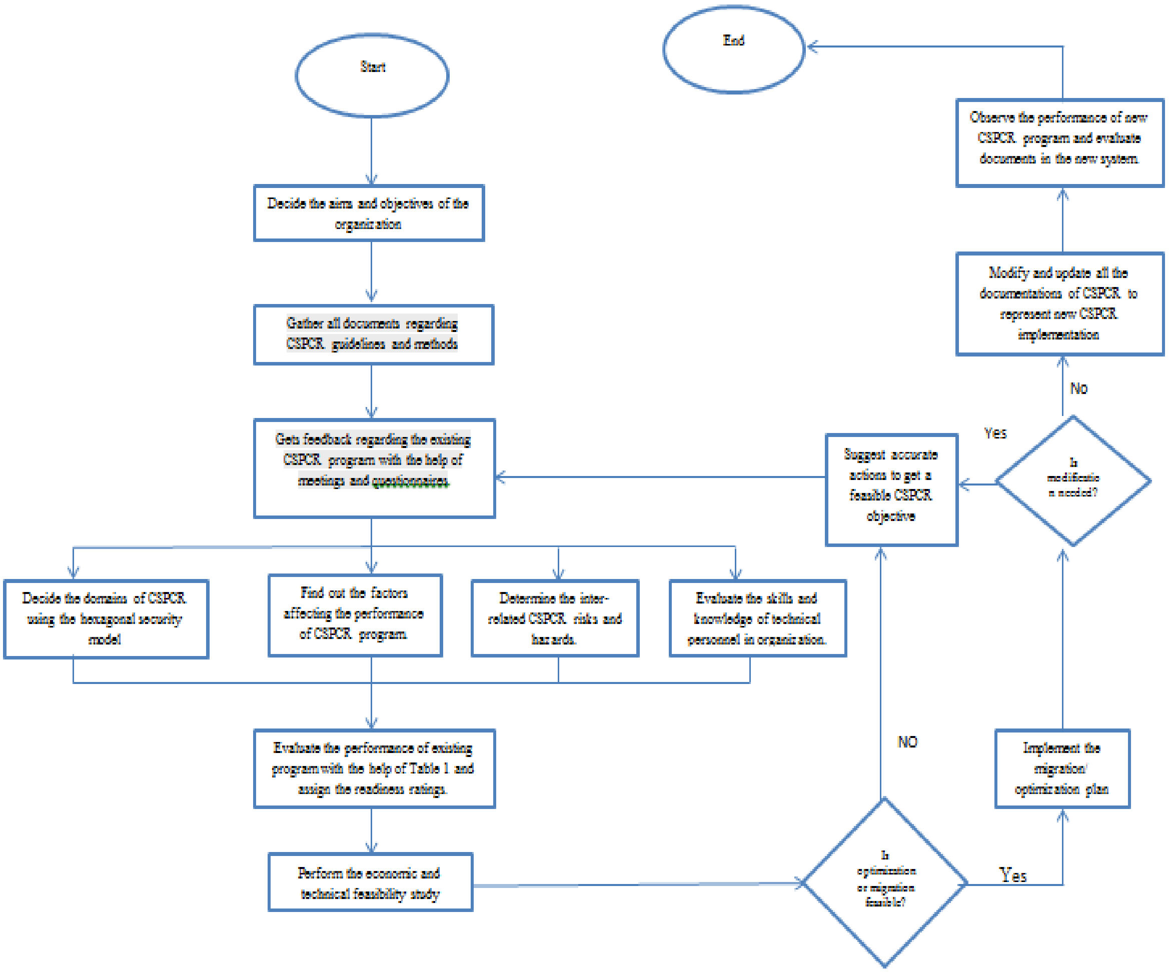
Start
End
Decide the aims and objectives of the organization
Gather all documents regarding CSPCR guidelines and methods
Gets feedback regarding the existing CSPCR program with the help of meetings and questionnaires.
Decide the domains of CSPCR using the hexagonal security model
Find out the factors affecting the performance of CSPCR program.
Determine the inter-related CSPCR risks and hazards.
Evaluate the skills and knowledge of technical personnel in organization.
Evaluate the performance of existing program with the help of Table 1 and assign the readiness ratings.
Perform the economic and technical feasibility study
Is optimization or migration feasible?
NO
Yes
Implement the migration/ optimization plan
Suggest accurate actions to get a feasible CSPCR objective
Is modification needed?
Yes
No
Modify and update all the documentations of CSPCR to represent new CSPCR implementation
Observe the performance of new CSPCR program and evaluate documents in the new system.

Figure 5. The CSPCR readiness model

REFERENCES

[1] Sagala, A., and Hutabrat R., "Private Cloud Storage Using OpenStack with Simple Network Architecture", *Indonesian Journal of Electrical Engineering and Computer Science*, pp. 155-164, 2016.

[2] Shen, Z., *et al*., "Cloud Computing System Based on Trusted Computing Platform", *2010 International Conference on Intelligent Computation Technology and Automation*, 2010.

[3] McEwen, A., and Cassimally, H., *Designing the Internet of things*, 2014, Chichester: Wiley.

[4] BSA Global Cloud Computing Scorecard, United Nations Conference on Trade and Development (UNCTAD) Information Economy Report (IER), pp. 103-103, 2013.

[5] "Multi-Cloud Governance Service based on Model Driven Policy Generation", *Proceedings of the 3rd International Conference on Cloud Computing and Services Science*, 2013.

[6] Huang, X., and Du, X., "Efficiently Secure Data Privacy on Hybrid Cloud", *2013 IEEE International Conference on Communications (ICC)*.

[7] Ahmed, S., and Kumaran, T., "Cloud Deployments Methods in Guarantee of Protection and Confidentiality Constraints", *Indonesian Journal of Electrical Engineering and Computer Science*, pp. 101-103, 2018.

[8] Instant Access to Gartner research on Cloud Security, Cloud Services, and the Hybrid Cloud. (n.d.). Retrieved from https://www.gartner.com/technology/topics/cloud-computing.jsp

[9] Sibiya, G., *et al*., "Digital Forensic Readiness in a Cloud Environment", *2013 African*.

[10] Kao, C. H., and Liu, S. T., "A Prototype System for Object Management in Private Cloud", *2011 International Conference on Cloud and Service Computing*.

[11] Reith, M., *et al*., "An Examination of Digital Forensic Models. International Journal of Digital Evidence", 2012.

[12] Martini, B., and Choo, K. R., "An Integrated Conceptual Digital Forensic Framework for Cloud Computing", *Digital Investigation*, vol. 9, no. 2, pp. 71-80, 2012.

[13] McKemmish, R., What is forensic computing? Trends & Issues in Crime and Criminal Justice, 1999.

[14] Kent, K., *et al*., "Guide to integrating forensic techniques into incident response", 2016.

[15] Hong, I., *et al*., "A new triage model conforming to the needs of selective search and seizure of electronic evidence", *Digital Investigation*, vol. 10, no. 2, pp. 175-192, 2013.

[16] Dilijonaite, A., “Digital Forensic Readiness”, *Digital Forensics*, pp. 117-145, 2017.

[17] Misljencevic, B., Cloud Platform Solutions: Data Classification for Cloud Readiness, 2017.

[18] [18] Quick, D., Martini, B., & Choo, K. R. (2014). Cloud Storage Forensic Framework. *Cloud Storage Forensics*, 13-21. doi:10.1016/b978-0-12-419970-5.00002-8

[19] Reid, R. C., and Gilbert, A. H., “Using the Parkerian Hexad to Introduce Security in an Information Literacy Class”, *2010 Information Security Curriculum Development Conference on - InfoSecCD '10*.

[20] Welton, T., IT Security for End Users: The CIA Security Triad, 2015.

[21] McKay, J., Pitching the Policy: Implementing IT Security Policy through Awareness, *SANS Institute*, 2013, Retrieved from www.giac.org/paper/gsec/3223/pitching-policy-implementing-security-policy-awareness/105199

[22] Vurukonda, N., and Rao, B., “A Secured Cloud Data Storage with Access Privileges”, *Indonesian Journal of Electrical Engineering and Informatics*, pp. 219-224, 2016.

[23] Alarifi, S., and Wolthusen, S. D., “Mitigation of Cloud-Internal Denial of Service Attacks”, *2014 IEEE 8th International Symposium on Service Oriented System Engineering*.

[24] Li, H., *et al*., “Byzantine-Resilient Secure Software-Defined Networks with Multiple Controllers in Cloud”, *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 436-447, 2014.

[25] Alemeye, F., and Getahun, F., “Cloud Readiness Assessment Framework and Recommendation System”, *AFRICON 2015*.

[26] Hussein, N. I., *et al*., “Security Migration Requirements: From Legacy System to Cloud and from Cloud to Cloud”, *Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation*, 2013.

[27] Nathuni, L., and Sahni, A., Lal's commentary on the Copyright Act, 1957 (Act No. 14 of 1957): With the Copyright (Amendment) Act, 2012 (Act no. 27 of 2012), The Copyrights rules, 2013 & Neighboring Rights, also International Copyright Order, 1999.

[28] Reddy, P., and Chandrashekaran, S. Create, copy, disrupt. India's intellectual property dilemmas. New Delhi: Oxford University Press India, 2017.