International Journal of Advanced Scientific Research
ISSN: 2456-0421; Impact Factor: RJIF 5.32
Received: 07-04-2019; Accepted: 11-05-2019
www.allscientificjournal.com
Volume 4; Issue 4; July 2019; Page No. 34-41

Information governance for the implementation of cloud computing

Sourav Mukherjee
Senior Database Administrator & PhD student at University of the Cumberlands Chicago, United States

Abstract
Information Governance has become gradually an important area due to the explosion of data in numerous formats at diverse levels of any organization. An Information Governance platform may have the capability to improve the data quality and may also support in leveraging strategic decision making. There is a growing trend to move the data from on-premise software to the new on-demand cloud-based solutions to support the growing needs of the business computing services which has the potential to lower the costs and mitigating the risks. Cloud computing is considered as a utility that is massively scalable and can be readily modified, the way we may control the temperature in the furnace using the thermostat which has the potential to save energy. There are many organizations that are investigating the Cloud to see if the application can meet their information Governance needs such as eDiscovery, compliance, law, security, risk management, records management, and business operations. Information Governance is a super-discipline that embraces components of several key fields as mentioned above (Robert F. Smallwood, 2014).

Keywords: Cloud, Information Governance, tenancy, security, scalability, thin client

1. Introduction
Information Governance for the Implementation of Cloud Computing
Organizations are migrating applications and storage to the cloud at a faster rate. Cloud computing let the users' access and use shared data and computing services and resources via the Internet or a VPN link which is encrypted for the security purpose. Cloud computing does not signify the transfer of assets or resources to upkeep any business, it also functions like a partnership association where at least two parties are engaged to attain a common benefit, and the risks and opportunities are divided among themselves. Like any other outsourcing venture, cloud computing brings with concerns related to the procuring entity's lack of knowledge of the activities outsourced. Over a period, the control of the infrastructure by the sourcing organization diminishes. Such a partnership is under the threats of the non-equal relationships as one of the parties is in a leading place, as it handles certain processes. This happens in the case of cloud computing, as this is extremely challenging to insource the services moved to cloud to bring back to the on-premise. Majority of the organizations, nowadays, essentially depend on IT. When IT and the business are associated in an organization, IT supplies what the business desires and the business can provide what the market desires. IT has become a deliberate function for most of the organizations, and it is imperative that IT and business are aligned. IT governance is one of the most desirable ways to attain IT in a business position. Therefore, IT governance is a necessary method which needs to be applied to cloud computing information security to manage the risks associated with cloud computing information security. This study developments the required knowledge by outspreading IT governance to cloud computing and information security governance. This paper has offered a study on applying information technology (IT) governance policies and processes for the application of a tenable cloud computing platform. IT governance is explained as a set of procedures intended to inspire actions that are reliable with the mission, strategy, and principles of the organization, the methods address several matters related to IT such as decision processes, rules, the assignment of responsibilities, and contribution rights for the stakeholder. Cloud deployments give users some sovereignty and freedom from their IT department, and IT departments are inspired to have immediate resources at their removal and eliminating few of the errands for infrastructure to focus on business applications. IT governance must be effective. To offer such effectiveness in the IT governance process, there must have a dependence on a couple of key mechanisms such as -

- IT steering committee
- Engagement of senior management in IT
- Corporate performance measurement systems

One of the principal goals of IT governance is to take decisions for investment and utilization of IT functions by focusing the question about how an organization should gain investments to its IT for the highest benefit to the entire organization.
Moreover, as the use of cloud computing for bringing IT functions becomes universal, organizations using cloud computing must efficiently smear IT governance to it. While cloud computing gifts wonderful opportunities, it emanates with several risk factors as well. Information security is one of the highest risks in cloud computing. Thus, IT governance must be pragmatic to cloud computing information security to facilitate managing the risks associated with cloud computing information security. Cloud computing in the newest model to deliver the IT services and it demands a framework for securing the organization's information while stored in the cloud. Managers and IT leaders who are the subscribers of the Cloud-based services are held responsible for providing seamless IT performance.

Several critical IG challenges connected with cloud computing must be focused on. These take account of privacy and security matters, records management (RM) problems, and compliance questions, such as the competence to reply to legal discovery orders. Furthermore, there are metadata management and supervision questions. An inquiry and examination are required to perform to know how the Cloud Services providers will provide RM capability which is again a crucial matter to know how to lend support to IG functions such as archiving and e-discovery, and meeting IG policy requirements. Organizations need to identify the security risks, loopholes with regards to cloud computing and they should have a defined IG policy and controls in place to influence the Cloud technology to support electronic data and information being looking further on the Cloud Strategy.

With the growing maturity and expansion of cloud computing, public cloud computing services are an expected choice for enterprises to attain better cost savings and resource use, however, there are qualms about the security in the cloud computing services space.

Besides, enterprise data security and privacy questions have become one of the major factors that have delayed the popularity of cloud computing [4]. Thus, cloud computing will advantage from a defined framework of IT governance and the related best practices.

Cloud Computing

Cloud Computing is a new entrant in the field of Information Technology. At the core, the cloud technology offers a secure, hosted and customizable services over the internet. This is a substitute for running them on a personal computer, server or corporate network. Applications and on-demand resources/features such as data centers, applications, networking, storage, software, and analytics are all available. It is also a shared infrastructure that offers dynamic access to computing services. We only pay for what we use, and it is possible to easily scale up or scale down to match the user needs. It throws away the need to procure server hardware and creates a seamless process to deploy IT infrastructure to provision computing resources and creates a gateway for users to access applications, data, and storage within their own business unit environments or networks. Currently, cloud computing has befitted a global trend, and it has pulled the attention, concentration, and awareness from both the business unit and the academic society as well. Such technology provides a paradigm shift in the field of information technology. Thus, the corporate information resources would be stored, recovered, and administered on the cloud computing platforms. Possibly the greatest feature of all is that the services managed by the cloud provider can be easily turned on or off, increased or decreased, based on user needs.

Per the Forbes magazine contribution by Louis Columbus (Jan 7, 2018) says that [3], "83% Of Enterprise Workloads Will Be in The Cloud By 2020". The Logic Monitor's survey predicts that 41% of enterprise workloads will be run on public cloud platforms (top providers such as Amazon AWS, Google Cloud Platform, Microsoft Azure, IBM Cloud, and others) by 2020. An additional 20% are forecasted to be private-cloud-based followed by another 22% running on hybrid cloud platforms by 2020. On-premise workloads are projected to diminish from 37% today to 27% of all workloads by 2020. Considering the above factors, we can easily identify the extreme growth of the Cloud-based platform is coming to soar in the near-term.

The following picture (sources: Wikipedia [1], will demonstrate a conceptual overview and understanding of Cloud Computing showing the various elements involved in the Cloud (components). Cloud computing allows convenient, on-demand network access to a shared
pool of configurable computing resources that can be quickly provisioned.

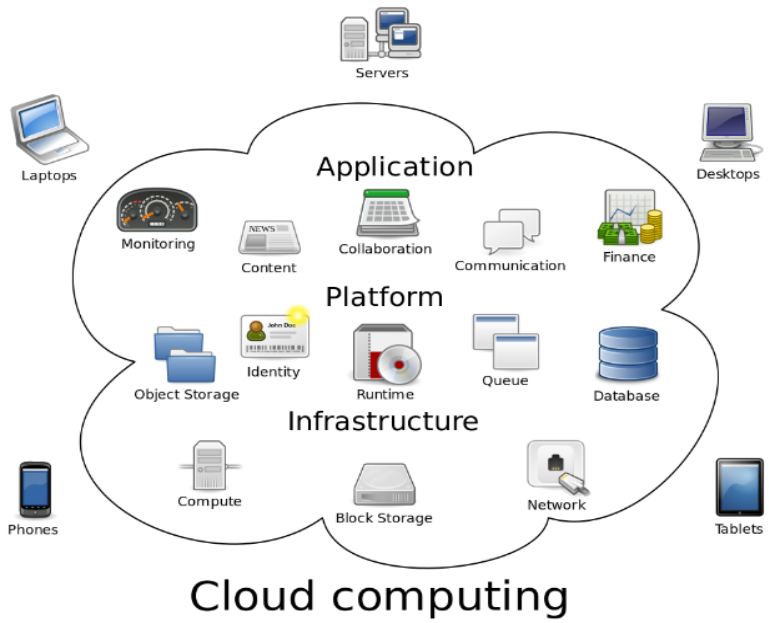

Fig 1: Cloud Computing [2]

The National Institute of Standards and Technology (NIST) is the official central arbitrator of
definitions, standards, criteria, rules, and guidelines for cloud computing. NIST defines cloud computing as [7]:

"a model for allowing convenient, ubiquitous, on-demand network admittance to a shared pool of configurable

computing resources such as networks, servers, storage, applications, and services that can be quickly provisioned and released with negligible management effort or service provider collaboration."

Key Features of Cloud Computing

NIST has defined five major characteristics of Cloud Computing.

Table 1

Features	Definition/details
On-demand self-service	Can provision the computing resources (CPU, memory, disk) automatically as needed based on the resource usage stats and that too without involving any human intervention.
Broad network access	Capabilities are available over the network, can be accessed via mobile phones, laptops or through other handheld devices (both thick and thin client platforms)
Resource Pooling	Multi-tenancy model is formed. Location independence with no control or knowledge about the exact location of the resources.
Rapid Elasticity	Quick scale-out and scale-in features provided. Resources may be provisioned as an unlimited capacity and maybe purchased at any time by any quantity.
Measured Service	Resource usage may be observed, measured and reported. Creates transparency for both provider and consumers.

"Gartner Projects Cloud Services Business to Grow Exponentially Through 2022. The worldwide public cloud services market is projected to rise 17.5 percent in 2019 to a total of $214.3 billion, up and about from $182.4 billion in 2018, according to Gartner, Inc [11]". Today there is no vendor or service provider whose business model offerings, services and revenue growth are not prejudiced by the cumulative growth and adoption of cloud-first approaches in the organizations. Through 2022, Gartner's study predicts that the market size and growth of the cloud services business at closely three times the development of overall IT services". Gartner further expects that by the close of 2019, more than 30 percent of Information technology providers' new software investments will shift from cloud-first to cloud-only. This means that license-based software consumption will further plummet, while SaaS and subscription-based cloud consumption models continue their rise.

Table 2: Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

Cloud Based Service Platforms	2018	2019	2020	2021	2022
Cloud Business Process Services (B PaaS)	45.8	49.3	53.1	57.0	61.1
Cloud Application Infrastructure Services (PaaS)	15.6	19.0	23.0	27.5	31.8
Cloud Application Services (SaaS)	80.0	94.8	110.5	126.7	143.7
Cloud Management and Security Services	10.5	12.2	14.1	16.0	17.9
Cloud System Infrastructure Services (IaaS)	30.5	38.9	49.1	61.9	76.6
Total Market	182.4	214.3	249.8	289.1	331.2

B PaaS = business process as a service;
PaaS = platform as a service;
SaaS = software as a service;
IaaS = infrastructure as a service;
Note: Totals may not sum up due to rounding factors.
***Source*:** Gartner (April 2019)

Few examples of business applications that commonly are migrated to the cloud environment include advertising, collaboration, e-mail, office productivity applications (Office Suite based products), sales support solutions (CRM based applications), customer response systems, file storage and shared locations, files (dropbox.com, SkyDrive, OneDrive) and system backups images. So knowingly, unknowingly we are keeping our corporate personal or important details to cloud-based systems. The mobile phone backups are mostly kept in Cloud-based storage (an example). This is totally ungoverned information stored in the cloud.

Cloud Deployment models

There are four basic cloud computing models which are popularly used depending on the customer's use cases – private, public, community, and hybrid combination of multiple clouds).

Table 3: Cloud Deployment models

Model	Purpose
Private Cloud	Dedicated to a single enterprise. Not shared. Mostly useful for such industries where the data is critical and sensitively such as healthcare, Insurance, Government sector, defense, etc.
Public Cloud	Managed by a general public or by a large industry group which is owned by the organization selling the cloud-based services.
Community Cloud	In this model, the cloud-based infrastructure is shared among several organizations which support or functions a specific industry/community with shared concern, mission, policy, etc.
Hybrid Cloud	This cloud model is a combination of two or more cloud models (for example, load balancing across the clouds).

According to the survey conducted by Right Scale [13], both public and private cloud adoption have improved as compared to the last year. The survey illustrates that the number of respondents now implementing public cloud is 92 percent. Consequently, the overall portion of respondents consuming at least one public or private cloud is today 96

percent.

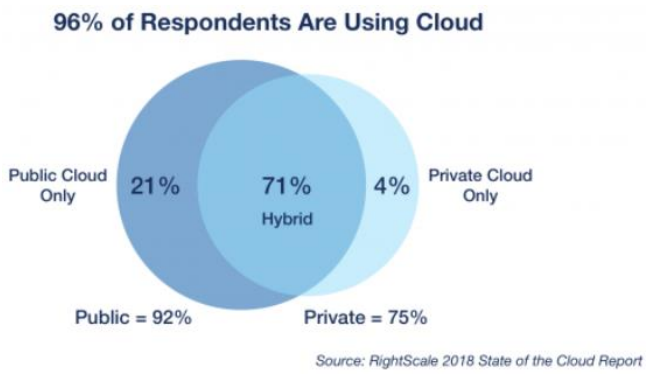

Fig 2: Public and Private Cloud Adoption Ratio [12]

Benefits of the Cloud

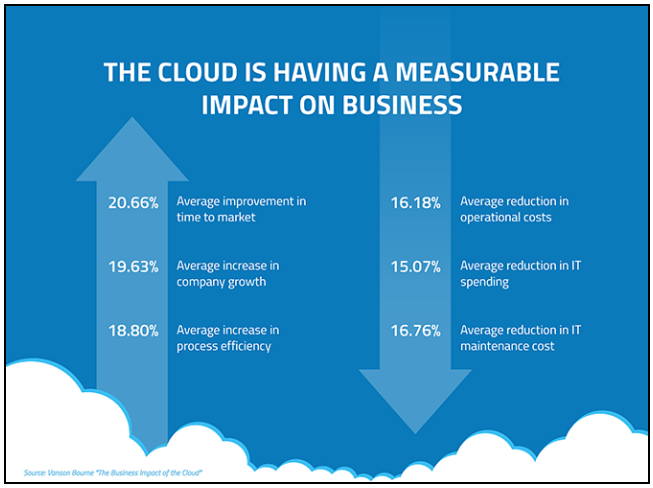

Fig 3: Cloud impact on business [15]

List of key benefits an enterprise can expect while adopting Cloud Infrastructure.

- Cost Reduction. The company does not have to spend a lot of money in procuring and maintaining the hardware, infrastructure. It can also help to reduce potential downtime.
- Scalability. This is the greatest advantage of the Cloud. Cloud Solutions offers a great deal of business to such organizations which are growing or have fluctuating bandwidth requirements [12]. If the business demand increases, increasing the resources at scale, and during off reason, maintaining the resource utilization tightly by reducing the resources. This approach significantly reduces the operational issues, maintenance, and Zero up-front investment.
- Data Privacy/Security. Cloud offers a variety of security features that may guarantee that Cloud offers a variety of security feature data is securely stored and handled. Cloud storage vendors implement baseline protections to the platforms and the data they manage, such as authentication, access control, connection and encryption [12].
- Mobility. Cloud Computing also offers mobile access to corporate in-house data through smartphones or via other digital equipment such as PDAs. Through the boon of cloud computing employees does not necessarily have to be present in the office to check the emails and knowing the corporate affairs. Moreover, if the company offers secured access through mobile, nowadays, employees can even monitor the alerts and respond to the alerts from anywhere.
- Disaster Recovery. Cloud-based services deliver rapid data recovery during any kinds of emergency situations - from natural disasters to power outages.
- Control. Cloud enables users having complete prominence and control over the data. We can easily choose which users need what level of access to what data and how long.
- Improved Collaboration. It allows discrete groups of people to meet virtually and effortlessly part information in real time and via shared storage.
- Less environmental impact. Companies who use shared resources improve their 'green' identifications [15].

Must have Cloud Computing Security Features

According to statistics cited by the Economist [14], "the average time involving an attacker breaching a network and its owner observing the intrusion is generally a period of 205 days." During that time, hackers can do indefinable damage to the business and the customers.

Implementing a strong security feature can be excessively expensive for the corporation making the investment. Using a cloud service provider can remove the large, up-front capital expenditures attached to top-of-the-line cybersecurity events.

- Strong Firewall which has the capability to monitor granular basis the file packets do traverse between source, destination.
- Intrusion Detection Systems (IDS) with proper Event-logging feature.
- Data at rest encryption and Data in transit encryption
- Internal firewall to safeguard the individual applications and the databases.
- Maintaining strong security at the data centers to avoid incurring threats through inside attackers. Tight monitoring is expected through CCTV monitoring, Biometric security controls and through armed security patrols throughout the time.

However, it's vital for businesses to make sure that the cloud service provider has the right security features for their cloud infrastructure.

When researching cloud service providers, check for the following 5 must-have cloud computing security features and services:

Besides the obvious benefits of using Cloud, there are few of the specific benefits offered by Cloud Computing Solutions are listed below:

- Bring Your Own Device (BYOD). If the users have access to an Internet connection, they can use any device to access the applications deployed in the Cloud Infrastructure.
- Cloud-based file storage solution provides a better and safer alternative as compared to storing data to unsecured removable media or sending details via the email address. Nowadays, any sensitive data can be uploaded via secured file transfer or secured email which no one other than the intended recipients can review or do anything.

Making Cloud Computing Governance Strategy Work [16]

The cloud needs a strict governance body that can deal with standardization of services and other shared infrastructure matters. The organization needs an interface to the group. The organization wants technology that can help automatically monitoring what goes on with the cloud. Along with interacting with the cloud provider(s), it is also required to monitor what the cloud providers are doing. Based on the situation, this may also require to be investing in technology that gets into cloud operations.

Many organizations use a dashboard, a kind of interface that holds the unlike

services and shows how if the performance measures up to the organization's goals. Few evolving vendors also deliver tools that let the companies monitor their cloud providers.

Many organizations also use a kind of service catalog as a record of IT services. This should be further extended to the cloud. The catalog may include evidence such as

- Whom to contact with regards to a service?
- Who has the right authority to change the service?
- Which critical applications are related to which service?
- Outages or any other incidents related to any service?
- Documentation of all agreements among IT and the customer or service users?

Cloud Computing Governance Principles [17]

Cloud computing governance to be based upon the following principles. They may be applied across the cloud lifecycle starting cradle to grave [17].

Table 3: Cloud Computing Governance Principles

Sr. No	Principle	Statement
1	Compliance due to Policies and Standards	▪ Be recognized and agreed upon at an early stage in the lifecycle. ▪ Conform with laws, regulations, and external policies concerning the collection, retention, and management of data with access to all stakeholders to applicable rules. ▪ Be detailed for all the architectural layers and applicable to all the stakeholders in the cloud ecosystem. ▪ A feasible exception plea processes must be in place to discourse any special circumstance.
2	Business Objectives to Drive Cloud Strategy	Both business and IT stakeholders must be engaged since the beginning in the decisions that influence the cloud transformation strategy and execution of specific cloud solutions.
3	Collaborative Contracts among Citizens of the Cloud Ecosystem	The governing rules must be evidently specified in a form that supports mutual understanding and agreement, such as a Memorandum of Understanding (MoU) or SLA that is obligatory within the scope and boundary of an enterprise, or a legally required contract that can be used and imposed across enterprise and government limitations. Stakeholders must represent the viewpoints of: • Key roles such as cloud service consumers, providers, integrators, developers, etc. • Crucial business functions like finance, legal, etc. A process for resolution of arguments among cloud service company providers must be in place.
4	Observance to Change Management Processes	Change comprises the original deployment of the cloud solution as well as its continuing maintenance and retirement. A confederated change management process is needed to organize change-related activities of the stakeholders in the cloud ecosystem.
5	Implementation of Vitality Processes to Attain Constant Improvement	Vitality smears to what is being governed. Continuous development of governance processes is furthermost effective when the areas being governed are flexible to changing requirements. Apposite infrastructure must be in place to efficiently monitor cloud computing governance procedures.

Thin Client solutions through Cloud Computing [18]

A Thin Client is a lightweight, cost-effective device which originates support from a server to leverage IT functions. The features for example applications, data, and memory which are there in PCs are kept in a safe data center while using this endpoint. The purpose of this design is to help the end users' access to virtualized desktops and the applications in the VDI. The overall ecosystem is broadly known as the Thin Client model. The kind of flexibility, agility, security, and supportability which this computing model offers are the major source of reason to be adopted rousingly in the digital age. It further lessens administrative workloads because tasks such as security plans and policies; and software upgrades can be applied at the data center. This results in fewer downtime and increases productivity amongst both the IT department and to the end users.

Virtualization supports all three major platforms of cloud computing resources such as private, public and hybrid. IT can associate Thin Client solutions with cloud computing to attain the required performance in VDI. The extraordinary capability and IT capacity of Thin Clients utilize the data-intensive characteristics of cloud computing through running complex applications. Though this smart approach, it is possible to deliver more scalable services through smart software tools and networking solutions.

Cloud Security Governance [19]

It refers to the management model that helps in delivering effective and efficient security management and operations in the cloud environment to attain the enterprise's business targets. This model integrates a hierarchy of executive mandates, performance expectations, operational practices, and metrics that result in delivering the optimization's business value for an enterprise. Cloud security governance technique answers a few leadership questions such as:

- Does our security investment produce the desired returns?
- Are we aware of our security risks and business impact?
- Are we increasingly dropping our security risks to the satisfactory levels?
- Are we able to establish a security-aware culture and mindset within the enterprise?

The strategic arrangement, value distribution, risk mitigation, effective use of resources, and measuring the performance are some of the key purposes of the IT governance model. It is important to recognize the operational culture and business and customer profiles of an enterprise to successfully pursue and achieve these objectives so that an effective security governance model can be customized for the enterprise.

In order to build a robust cloud security governance model

for an organization, it requires strategic-level security management capabilities in conjunction with the usage of right security standards and frameworks such as NIST, ISO, CSA, ENISA, COSO, ISACA and the implementation of a governance framework such as COBiT, ITIL, ValIT.

The immediate first step is to understand the overall governance construction, inherent components. A governance framework delivers referential leadership and best practices for setting up the governance model for security in the cloud. Suitable security standards and a governance framework are needed to be chosen based on the organizations' business objectives, targets, customer portfolio, and responsibilities for safeguarding data and other information possessions in the cloud environment.

IG threats and concerns in Cloud

With the benefits of cloud computing enterprises do not need to focus any longer to the IT services, rather they can focus more on the core business to increase the business. Since Cloud providers only host the hardware, infrastructure and software resources, the enterprise does not have to think about capital expenditure. Though the benefits of Cloud, the company can invest more in line with the business goals, objectives and focus on the core products, services, and Operations. Among the benefits of the Cloud, significantly there are IG threats and concerns which are described below.

- Short of clarity about ownership of information
- Managing records at the file level are not possible yet.
- Dealing with large failure and downtime associated with any cloud provider.
- Implementing legal holds during the situation of any litigation.
- Lack of Records Management functionality with most of the cloud-based applications.
- Limited capability to confirm that the cloud provider meets the duties to follow rules related to the governance of the information.
- Following countrywide data protection laws and rules such as GDPR [20], "personal information and important data protection system" defined by the Chinese government.
- Jurisdiction and political matters that may stand up since the cloud provider exist in outside of the organizations' geographic area.

Comparison of Cloud Computing Security Governance Frameworks

Table 4: Comparison: Security Governance Frameworks in Cloud Computing

Framework/Standard Governing Bodies	Policies and processes adoption (PPA)
International Standards Organization (ISO)	Process Management, and Security Management
The European Network and Information Security Agency (ENISA)	Recommendations, and creates checklists to achieve assurance
Organizations of the Treadway Commission (COSO)	Roles & Responsibilities, Enterprise Risk Management, and Process assessment model.
Information Systems Audit and Control Association (ISACA)	Business Process Management, Security Management
National Institute of Standards and Technology (NIST)	Cloud Reference Architecture. It is a non-regulatory agency
Information Systems Audit and Control Association (ISACA)	Business process management and Security management, benchmarking. ISACA developed a well-known IT governance framework which is popularly known as COBiT.
The Cloud Security Alliance (CSA)	Governance and Enterprise risk management

IG Guidelines for Cloud Computing Solutions [10]

Here is a set of guidelines defined which are aimed at helping the organization leverage cloud computing in a way to meet the business objectives without compromising the overall IG profile.

- Define the business objectives first. After that select the appropriate cloud provider which can meet the business objectives.
- During the project documentation phase, identify the appropriate roles and responsibilities related to the system and document the same way with details for any internally focused systems.
- In the project plan, to include the investigation and application of appropriate fixes section as described in the security threats with cloud computing section. During the phase, engage a good contract negotiator.
- Document high-level process and information flow subsequent to the Cloud computing projects. Address some of the key points, such as –
- How to migrate information, metadata from on-premise to cloud and vice versa?
- How to implement the legal hold on processes and practices?
- How to implement the Records Management capability or mass content migration if not supported by the provider? Apply alternatives, etc.

Cloud security concerns over Multitenancy environments [21]

Multi-tenancy is one of the keystones of modern cloud computing offerings. The concept was founded by Software as a Service (SaaS) vendors like Salesforce.com and slowly spread across the other cloud segments such as Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) systems.

virtual computing allows for multiple instances of an operating system and applications to be walled off from others that are running on the same computer. Essentially, each instance of the OS runs independently, as if it were the only one on the computer. This concept is primarily known as multitenancy. This concept has enabled the cloud service subscribers to empower more cost-effective shared, or pooled resources built on a single codebase. There are concerns which are raised by several vendors about scalability, access to better and newer features, support and security.

Appropriately designed and managed multi-tenant services can act even more securely than the traditional on-premise infrastructure as the vendor has the full sovereignty to the

system. Likewise, that discrete condominium units can be constructed in a secure manner with hard walls and robust locks in a shared community/infrastructure, multi-tenant cloud services can also be designed to partition user data and protect it against internal and external security threats and failures.

Conclusions and Future Study

Cloud computing acceptance is on the rise every year, and it doesn't take long to see why. Enterprises know and recognize the cloud computing benefits and understand how they influence their bottom-line (production, collaboration, security, and revenue). By adopting a cloud-based solution, an enterprise can stop a lot of problems that wave the organizations by relying on traditional on-premises infrastructure. Cloud implementation increases every year since companies understand that technology offers them access to outstanding enterprise technology. And, implementing a cloud solution today, may bring the organization ahead of the competitors. Now if the organization is leaned more towards the public, private or hybrid cloud is a substance of individual choice. One can only achieve the desired result when service providers guarantee reliability, elasticity, scalability, and billed usage. An organization's board and members are responsible and accountable to shareholders, regulators, and customers for designing and developing a suitable framework of standards, procedures, and activities that, together, make certain the organization is benefited securely from Cloud computing. Additionally, organizations must acclimate their existing IT governance to include cloud computing. IT organizations must show leadership to endorse information security governance, overwhelm user resistance, and develop a sound ethical framework that promises independence from external compulsion.

References

1. Author Jimmy Spencer, retrieve from https://securityfirstcorp.com/why-is-cyber-security-important/, 2018.
2. Johnston Sam. (n.d), retrieved from https://en.wikipedia.org/wiki/Cloud_computing#/media/File:Cloud_computing.svg
3. Columbus Louis. 83% Of Enterprise Workloads Will Be in The Cloud By 2020, retrieved from https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise workloads-will-be-in-the-cloud-by-2020/#7dfa12916261, 2018.
4. JE Mbowe, SS Msanjila, GS Oreku, K Kalegele, On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach, Journal of Software Engineering and Applications. 2016; 09(12):601-623.
5. Rahman Syed. Industry, Itii. Securing Cloud Computing Through IT Governance, 2019.
6. Loos Howard Components of Information Governance. Retrieved from http://armautah.org/wp-content/uploads/2016/11/Components-of-Information-Governance-presentation.pdf, 2015.
7. P Mell, T Grance, The NIST definition of cloud computing recommendations of the National Institute of Standards and Technology, NIST Special Publication, 2011, 145:7.
8. Fig 1: Author Tony Perez, retrieve from https://perezbox.com/2015/10/website-security-is-not-an-absolute/, 2015.
9. Fig 2: Author Susan Ranford, retrieve from https://www.ittropolis.com/physical-security-just important-online-security/, 2018.
10. Smallwood RF. Information governance: Concepts, strategies, and best practices John Wiley & Sons, 2014, 574.
11. Newsroom, Press Releases, Stamford, Conn. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g, 2019.
12. Bozicevic Vedran. Cloud Computing Benefits: 7 Key Advantages for Your Business. Retrieved from https://www.globaldots.com/cloud-computing-benefits/, 2018.
13. Weins, Kim. Cloud Computing Trends: 2018 State of the Cloud Survey. Retrieved from https://blogs.flexera.com/cloud/cloud-industry-insights/cloud-computing-trends-2018-state-of-the-cloud-survey/, 2018.
14. Must Have Cloud Computing Security Features (n.d). Retrieved from https://www.whoa.com/5-must-have-cloud-computing-security-features/
15. Coles, Cameron (n.d.). 11 Advantages of Cloud Computing and How Your Business Can Benefit from Them. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/11-advantages-of-cloud-computing-and-how-your-business-can-benefit-from-them/
16. Judith Hurwitz, robin bloor, marcia kaufman, fern halper (n.d.). how to make your cloud computing governance strategy work. Retrieved from https://www.dummies.com/programming/cloud-computing/cloud-computing-security/how-to-make-your-cloud-computing-governance-strategy-work/
17. Cloud Computing Governance Framework – Cloud Computing Governance Principles. Retrieved from http://www.opengroup.org/cloud/gov_snapshot/p5.htm
18. Clearcube Staff (n.d). What are the Different Elements of Cloud Computing? Retrieved from https://www.clearcube.com/posts/what-are-the-different-elements-of-cloud-computing/
19. Michael Addo-Yobo. Cloud Security Governance - Optimizing the Business Benefits of Security in the Cloud. https://www.coalfire.com/The-Coalfire-Blog/May-2018/Cloud-Security-Governance, 2018.
20. A Practical Guide to Data Privacy Laws by Country. Retrieved from
21. https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/
22. Kaplan, Jeff (n.d). Cloud security concerns persist over multi-tenancy environments. Retrieved from https://searchcloudcomputing.techtarget.com/answer/Cloud-security-concerns-persist-over-multi-tenancy-environments
23. Mukherjee S. Benefits of AWS in Modern Cloud. arXiv preprint arXiv:1903.03219, 2019.
24. Mukherjee S. Popular SQL Server Database Encryption Choices. arXiv preprint arXiv:1901.03179, 2019.
25. Mukherjee S. How IT allows E-Participation in Policy-Making Process. arXiv preprint arXiv:1903.00831, 2019.
26. Mukherjee S. How Stakeholder Engagement Affects IT

Projects. International, Journal of Innovative Research in Science, Engineering and Technology, 2019, 8(3).
27. Chakraborty, Moonmoon & Excellence, Operations. Supply Chain & Inventory Management. 10.6084/m9.figshare.7824107, 2019.
28. Mukherjee Sourav. Overview of the Importance of Corporate Security in business. 10.15680/IJIRSET.2019.0804002, 2019.
29. Mukherjee Sourav. How stakeholder engagement affects IT projects. 10.15680/IJIRSET.2019.0803265, 2019.
30. Chakraborty M. Fog Computing Vs. Cloud Computing. arXiv preprint arXiv:1904.04026, 2019.
31. Mukherjee Sourav. SQL Server Development Best Practices. International Journal of Innovative Research in Computer and Communication Engineering. 10.15680/IJIRSET.2019.0803266, 2019.
32. Mukherjee S. Indexes in Microsoft SQL Server. arXiv preprint arXiv:1903.08334, 2019.
33. Chakraborty Moonmoon. Planning, Control Systems and Lean Operations in Information Technology. 10.6084/m9.figshare.7886138, 2019.
34. Chakraborty Moonmoon. Managing Risk, Recovery & Project Management. 10.6084/m9.figshare.7886141, 2019.
35. Chakraborty Moonmoon. Operation improvements & quality Management in healthcare Operation Improvements & Quality Management in Healthcare. 10.6084/m9.figshare.7886144, 2019.
36. Mukherjee, S. The battle between NoSQL Databases and RDBMS.