SECP's Cloud Adoption Guidelines for Incorporated Companies /Business Entities

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

Table of Contents

Record of Amendments

This is a record of changes made to this document, based on review.

Rev	Approval Date	Document ID Code	Description of Change	Approved By
0.0	June'2021	G-CA4RC	First Approval	The Commissioner (ISD)

1 Overview

Cloud Computing is a technological framework which offers a convenient, on demand access to a shared poll of resources such as servers, storage, and applications, over the internet. Users don't require their own controlled hardware or software. Instead, these resources are maintained and provided by cloud service providers; user can get access to these resources over the internet by paying nominal charges to the cloud service providers. Cloud computing had been proved very useful in different sectors. In business entities (i.e. corporate entities registered with SECP) cloud computing offers numerous benefits including: better resource utilization, scalability, business continuity, improved collaboration and speed to market etc. From small scale single member incorporated companies to large scale listed companies, everyone is continuously using services offered by cloud service providers. Building an information technology (IT) infrastructure can be incredibly complex and expensive for new and growing businesses entities. Limited resources, expertise, and time often constrains how much small and midsize enterprises are able to accomplish. Software companies have considered this demographic by building out tools that are either specifically designed for BEs or can be configured to support more modest needs. Whether we're discussing email marketing or accounting tools, there's a service that can meet your needs regardless of your company's economic and technological thresholds. Every business uses the services of cloud according to their scale.

1.1 Purpose

This guideline will provide all business entities (Bes) incorporated with SECP the flexibility to decide, upon their needs and requirements, which applications, data, and resources can be put in the appropriate cloud service and deployment model. Therefore, in co-ordination with relevant authorities and stakeholders, the SECP issues these **Cloud Adoption Guidelines** to encourage cloud adoption by all BEs incorporated with SECP, aiming to provide guidance for all regulatees to use in their transition to cloud computing. This also allows indigenous industry to benefit from global data sets by identifying actionable intelligence and vulnerabilities to make impactful decisions.

1.2 Scope

These **Cloud Adoption Guidelines** will be applicable to all BEs incorporated with Securities and Exchange Commission of Pakistan under the Companies Act 2017, Securities Act 2015, Insurance Ordinance 2000 and NBFC Regulations 2008 etc. BEs incorporated with SECP but supervised by sector specific regulators need to ensure compliance with sector specific guidelines on Cloud based services by their regulators. These guidelines pertain to all new IT investments which are to be made by any regulatee, as well as for migrating legacy applications and data to cloud. These Guidelines will become effective from June 1, 2021; however, earlier adaption is encouraged.

1.3 Adaptation of Cloud in BEs

A Business Entities (BEs) incorporated with SECP is an organization that would typically have many employees. These business owners are well aware of cloud computing. They have adopted cloud computing for its economies of scale, ease of use and low cost. Many BEs have been on the leading edge of public cloud advocacy and adoption. Cloud facilitate in reducing/eliminating capital expenditures (Capex), gives flexibility to launch or scale a business; however, it will be a business decision of the BEs based on control on their data and cost savings in the short vs long term.

2 Public Cloud Adoption Phases

There is a strong demand for cloud adoption by BEs for cloud-based server capacity, information and database management, security, system and user access management, ERP, CRM and collaboration tools. Figure below shows the phases that one has to go through while selecting and transitioning the services to cloud. Throughout the adoption process, BEs need to focus on the areas of trust, security, legal, compliance and organizational issues.

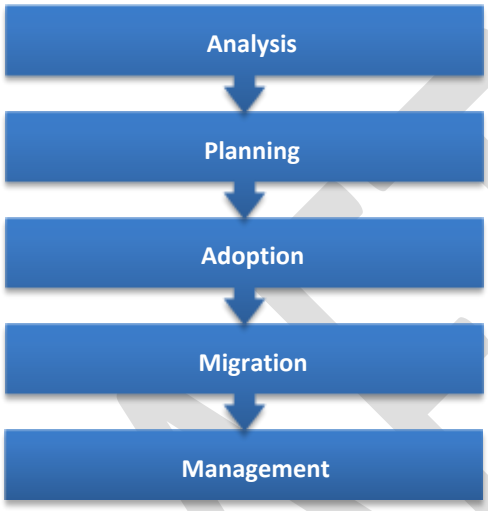

Figure 2: *Cloud Adoption Phases by BEs*

2.1 Analysis Phase

Analysis phase is the first phase. While adopting cloud in BEs, the BEs must first analyze the need to use the cloud and at what extent the company is able to shift to cloud and able to bear the cost of cloud services. BEs must also identify possible cloud application candidates such as, the impact of migrating to the cloud and do an analysis of the existing systems, applications and business processes.

2.2 Planning

Planning is the most crucial phase in adoption before purchasing of any cloud services. Planning phase helps to set the direction and objectives for adopting cloud computing. The management team of BEs chooses the platforms for deployment and the infrastructure finance, plans, security and legal issues. Improper planning may lead to increase in cost or unsuitable establishment of required services.

2.3 Adoption

Adoption phase is concerned with purchasing of the services planned during planning phase. In this phase, firstly the vendor for the particular service is selected and these services are taken from selected cloud vendor. In this phase, work on application integration with cloud platforms and infrastructure, outsourcing strategies, SLAs, security policies and legal compliance management is done. This phase sets the stage for migration of the selected applications and systems to the cloud.

2.4 Migration

After adopting the cloud services from vendors, the BEs requires to shift their working over cloud services. Migration phase helps with migration of user data and application to the cloud. The users

start using the cloud services. The management must ensure adequate technical and user support during the migration process.

2.5 Management

Management is the last phase and is ongoing process that never ends. This phase involved to identify document and evangelize best practices. The cloud platform and services must be adequately maintained. Local and remote support and monitoring teams must be put in place.

3 SECP Guidelines for BEs to Ensure the Needs for Cloud

While performing the planning in adoption of cloud in business, every individual in business have their different opinions. Overall, respondents willing to consider purchasing of cloud solutions and needs are recorded and considered to identify the actual requirement of cloud adoption in business. The BE must have to understand how to gain access to the services and get huge benefit by using these services of cloud. Following are different guidelines for BEs to ensure that they get the most out of their cloud.

3.1 BE's Cloud Governance Body

A well-defined governance structure must be in place to ensure smooth implementation and optimal results. A body should be constituted at the BE's board level for adoption and defining responsibilities related to operational aspects of cloud-based applications/ services.

a. Setting the guidelines for the policy defining the objectives, scope, governance as well as implementation framework to be adopted;
b. Driving cloud adoption across the organization through simplifying procurement processes for Cloud solutions;
c. Checking technical and commercial requirements to decide on Cloud viability for new IT investments and migrating legacy applications and data to cloud;
d. Checking security requirements to decide on Cloud viability for new IT investments and migrating legacy applications and data to cloud;
e. Setting the cybersecurity requirements and guidelines; and ensuring compliance with these requirements such as: anonymized or data-encryption etc.;
f. Ensure defining data classification criteria in line with domain specific data classification requirements.
g. Setting up SLA requirements and guidelines such as: how to terminate contract, moving of data ensuring full control over data without any binding whatsoever; and ensuring compliance with these requirements etc.;
h. Supporting coordination across different governance bodies and enabling the ecosystem through securing budgets for Cloud adoption as well grooming ICT experts with Cloud technical expertise.

3.2 Start small

The BE must first provide time employees to get familiar with the services provided by cloud. This can be possible by using single application at a time and by giving some weeks for employees to get accustomed to the environment. Once they are at ease, BE can add more cloud services to train employees completely by the services offered by cloud.

3.3 Think Big

While purchasing the services of cloud, BE has to ensure that the cloud services adopted by it can be scaled up to a desired level across time zones, types of services and can serve employees and customers alike. If they cannot, then organization required to keep looking for required services.

3.4 Ability to Export data

The BE must purchase such type of cloud services which is able to export in different standard formats mostly used by the BE so that BE can be able to shift to different clouds according to the requirement or can be able to backup the data at different cloud servers. For this, the BE required to export their data to common applications such as Microsoft Word/Excel or database files for Oracle, MySQL etc.

3.5 Data Classification

Data classification is the process of organizing data by relevant categories so that it can be utilized according to its sensitivity and criticality. BEs will likely have vastly different types of information and that information will be associated with varying levels of sensitivity. Data classification provides a tool to determine and assign relative values to the data BEs possess and generates. A simple and clear data classification framework is essential for BEs as they move to the cloud to ensure they can receive the critical benefits of cloud computing in a cost-effective way. This ultimately enables individual decision makers to understand better what types of data can be stored on each type of cloud system architecture. The BEs may follow three simple classifications of data as:

3.5.1 Non-confidential data

Data relating to routine BEs, operations and services. This is the data that is publicly available.

3.5.2 Sensitive official data

Information not intended to be published, which shall be accessed only by certain people having proper authorization and which justifies moderate protective measures.

a. Phone numbers, registration numbers (BVN, vehicle etc.), passport.
b. Information that contains at least one personally identifiable information (PII) like name (first and last), address, biometrics etc.
c. Data classified as “confidential” and, perhaps, certain categories of “secret” data (e.g. Obsolete or archived “secret” information).
d. Information accessible through an Intranet only, but available to broadly defined categories of authorized officials and public servants. Drafts of laws and regulations that are not yet in the public domain.

3.5.3 Secret/Classified data

Secret information requiring the highest level of protection from serious threats, whose breach will likely cause threats to life or public security, financial losses, serious damage to public interests etc.

a. Lead directly to widespread loss of life.
b. Threaten directly the internal stability of Pakistan or friendly nations.
c. Raise international tension.
d. Cause exceptionally grave damage to relations with friendly nations.

e. Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.
f. Cause long term damage to the Pakistani economy.
g. Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.

3.6 Data Classification Consideration while adopting Cloud computing options

BEs are required to consider following, while adopting Cloud computing options:

a. Classify all BE data into different levels depending on their level of sensitivity or security protection requirements.
b. Opt for cloud service providers according to the data classification i.e. the more the sensitive data is the more secure or protected cloud service should be relied upon only if the technical requirements are met.
c. Ensure customer data protection and take all "reasonable" steps needed to secure it.
d. For organizations own data any secure cloud service provider may be relied upon, if the technical requirements are met.
e. In the case of government data, only government approved cloud service providers should be relied upon, if the technical requirements are met.
f. In the case of Personally Identifiable Information (PII), only most secured cloud service providers should be relied upon, if the technical requirements are met. For example: BEs need to encrypt the data and ensure that the key and encrypted data is not stored on same cloud. The objective is to ensure that no two-separate set of data are present on same cloud as it may result in identification of the person.

3.7 Service Level Agreement (SLA)

The Service Level Agreement (SLA) describes the refund for service outage, termination procedures, fees, backup and Business Continuity Planning (BCP) that will be provided by the vendor. BE must read and understand the terms to know the impact of the usage of cloud services in business of the organization.

3.8 Inexpensive Cloud Options

Several free cloud computing options exist for emails, document management and even CRM and ERP. BE just need to pay only its usage exceeds in number of user count or storage space. Some cloud services providers also offer the free trial periods to the users. The BE must review services before deciding to buy these services.

3.9 Ensure Compliance

Assess if the cyber security requirements, which are based on the Pakistan Cloud First Policy 2021, National Cybersecurity Policy 2021[1], sector specific guidelines, authentication requirements and other specific cyber security measures and regulations are met by the Cloud model under consideration.

[1] drafted

All business entities, while selecting Cloud Service Providers, must ensure that selected service provider does not offer the services through their data centres located in any hostile country i.e. (India, Israel, etc.)

Table of Abbreviations & Definitions

Abbreviation / Term	Full Word / Definitions
SECP	Securities & Exchange Commission of Pakistan
BEs	Business Entities
ICT	Information and Communication Technologies
SLA	Service Level Agreement
Cloud	According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."
CSP	A cloud service provider (CSP) is a third-party company that offers components of cloud computing such as infrastructure, software, storage, application etc.
Public cloud	Cloud infrastructure provisioned for open use by the general public. This cloud model may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It can be located anywhere but should have any local partner CSP. Resources of the cloud infrastructure can be shared by any number of organizations.
Government cloud	Cloud infrastructure provisioned for use by government organizations only. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It can only be located in Pakistan. Resources of the cloud infrastructure can be shared by Government organizations only.
Private cloud	Cloud infrastructure provisioned for exclusive use by a single organisation. It is managed and operated by the organisation, a third party, or some combination of them. It may be located anywhere and can be on premise or off premise cloud. Resources of the cloud infrastructure are used by a single organization.
Hybrid cloud	Hybrid cloud is a solution that combines one or more cloud services. It allows data and applications to be shared between them. An organization can store its sensitive data on one type of cloud whereas public data on another, thus taking care of its security needs as well as leveraging the robust computational resources of a public cloud.
Cloud computing service models	Cloud computing service models are: SaaS, PaaS and IaaS
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., Dropbox, iLearn, and MS O365).
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider (e.g., Amazon Cloud Service, Microsoft Azure).
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party (e.g., Amazon Cloud Service, Microsoft Azure).
Personally, Identifiable Information (PII)	Personally identifiable information, is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address etc.