Annex 4

Cloud Adoption Lifecycle

1 CLOUD ADOPTION LIFECYCLE

The adoption of cloud services involves the migration or relocation of application data and platforms to a cloud based environment. Based on the specific requirements of government organizations, the migration plan may entail either from an on-premise environment to a cloud environment or moving from an existing cloud solution to another i.e. Cloud-to-Cloud Migration.

Government organizations are advised to follow the lifecycle as mentioned below to successfully deploy a cloud service within the organization.

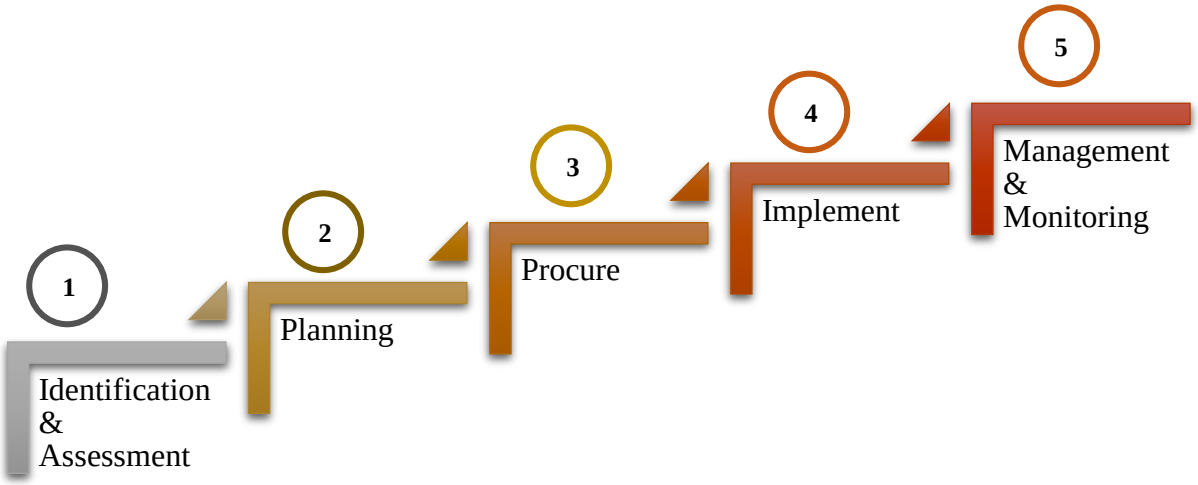

Figure 1: Stages of Cloud Adoption Life Cycle

The key activities associated with each stage in the adoption lifecycle are as follows.

1.1 Identification and Assessment

The guidelines outlined in the sections below would assist Government organizations to identify and assess the cloud migration need in consideration of the best practices to be followed prior to cloud adoption.

1. **Analyze the organization's work scope and IT objectives** along with current IT workload housed either in in-house data centers or external data centers and **identify the benefits** which make cloud adoption essential.

2. Perform a **Cloud Readiness Assessment**[1] to assess the cloud readiness of the organization's IT workload to be deployed in a cloud environment.

[1] Assists Government organizations with a gap-analysis of the existing application landscape; Technical Feasibility, Risk Assessment, Strategic Alignment, and Cost Assessment in order ensure a smooth migration.

3. The existing IT applications in a Government organization should be assessed based on the following criteria.

    a. Technical feasibility assessment
    b. Risk assessment
    c. Strategic alignment and cost assessment

4. Perform an **Application Assessment** to evaluate the existing IT applications to determine the low risk and easier ones to be migrated first i.e. applications with lesser dependencies on other applications or external systems.

    Government organizations are advised to perform the assessment via adhering to the following guidelines.

    a. Create an application inventory
    b. Identify application dependencies
    c. Prioritization of applications (based on the criticality, complexity and associated risks)

5. **Infrastructure Assessment** of the selected cloud service provider.

6. Ensuring the **availability of a secure network connectivity** between the office premises of the Government organization and the preferred cloud platform.

7. **Evaluate the current compute storage and database capacity** consumed by the existing servers.

8. Analyze **current utilization and the capacity requirements of applications** to be migrated.

9. Analyze the **CPU and memory usage during the peak times**.

1.2 Planning

A structured planning is required by the Government organizations to adopt cloud, which includes understanding the criteria for evaluating the CSPs, performing the capacity sizing estimation for Compute, Storage and Network and selection of suitable cloud models for migrating the existing applications as well as ensuring workforce readiness for cloud adoption.

Government organizations can adhere to the following guidelines to successfully get through the planning stage.

1. Conduct a '**Cost/Benefit Analysis**' on adopting a cloud service. Analysis must include value for money, fitness for the purpose, a clearly defined business case, total cost of ownership (TCO), asset impact, organizational impact, and technical environment impact.

2. Perform a **capacity sizing of the existing IT applications and infrastructure** for storage, network and security, compute.

3. Evaluate and select the most suitable **cloud service model** for the organization from the following three cloud service models.

   a. Infrastructure as a Service (IaaS)

   The most basic category of cloud computing services. It allows one to rent IT infrastructure i.e. servers and virtual machines (VMs), storage, networks, operating systems, from a cloud service provider on a pay-as-you-go basis.

   b. Software as a Service (SaaS)

   Software as a service is a method for delivering software applications over the internet on demand and typically on a subscription basis. Under SaaS, cloud providers host and manage the software applications and underlying infrastructure, and handle maintenance activities such as software upgrades and security patching. Users connect to the application over the internet, usually via a web browser on their phone, tablet, or PC.

   c. Platform as a Service (PaaS)

   Platform as a service refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development.

4. **Classification of data** in alignment of the Sri Lanka Government Information Classification Framework[2] and deciding on data to be processed in and out of the territorial boundaries of Sri Lanka[3].

5. Define the **roles and responsibilities** of each stakeholder such as Cloud Service Provider, Managed Service Provider and Government organization for proper demarcation of roles and responsibilities of each stakeholder.

[2] Refer Annex 7 : Sri Lanka Government Information Classification Framework
[3] Refer Annex 2 : Legal Landscape on Cross Border Data Flow

6. Perform a comprehensive '**Skill Gap Analysis**' to identify the current proficiency level of the staff in cloud hosted services and develop strategies to bridge the identified skill gaps.

    a. The organization's Chief Digital Information Officer (CDIO) is responsible for conducting comprehensive workforce planning and ensuring the availability of appropriate learning and development opportunities to ensure a digitally competent workforce with the right skills and knowledge.

7. If a Government organization has hired a 3rd party vendor for application development, hosting and service maintenance; same should be supported with a duly signed and valid agreement. And Government organizations are responsible for maintaining continuity, updates and renewal of such agreement in accordance with their requirements.

1.3 Procure

Upon finalizing the capacity sizing and selection of a suitable cloud model, the Government organizations need to focus on the procure stage. The section outlines the guidelines to be followed by Government organizations in procuring cloud services from a Cloud Service Provider.

1. Ensure that the selected service provider satisfies the following conditions.

    a. Fit for the purpose
    b. Adheres to local legal, procurement and regulatory guidelines
    c. Provides adequate risk management for information and ICT assets as defined by the relevant security principles, and

2. Take extra care to prevent '**Vendor Lock-in**' when procuring the service and ensure flexibility for future platform migrations.

3. The adoption of cloud services should be supported with **a business case**, approved by the higher management of the organization. The business case must include;

    a. A summary of the intended cloud solution including the purpose and anticipated benefits.
    b. Required application architecture, operating system, technology etc.
    c. An assessment of security risks and mitigation actions depending on the information sensitivity and classification

d. A user manual explaining the operational framework and support functions (including responsibility matrix, SLAs, KPIs, processes, procedures etc.)

4. Discuss with the cloud service provider and ensure the availability of the following critical elements to guarantee a seamless and successful cloud adoption journey.

   a. Technical Support: Round-the-clock access to knowledgeable technical experts to promptly address any cloud-related issues.

   b. Technical Architecture: A well-defined and documented technical architecture that aligns with the organizational objectives and requirements.

   c. Service Level Agreements (SLAs): Clearly defined and measurable SLAs that guarantee consistent service uptime, performance benchmarks, and prompt response times.

   d. Maintenance: Proactive and comprehensive maintenance plans to maintain optimal performance, stability, and security.

   e. Responsibility Matrix: A clear and unambiguous delineation of responsibilities between the service provider and the Government organization, ensuring accountability and streamlined issue resolution.

   f. Technical Account Manager (TAM): A dedicated TAM to serve as the primary point of contact for the Government organization, advocate for the organization's cloud needs, providing ongoing guidance and support.

5. Ensure that the selected CSP owns and maintains a **Tier 3**[4] **certified data center facility** capable of accommodating the following

   a. Multiple paths for power and cooling, and redundant systems that allow the staff to work on the set-up without taking it offline.

   b. No need of a total shutdown during maintenance or equipment replacement

   c. A back-up solution that can keep operations running in case of a local or region-wide power outage.

   d. Ensure that the equipment can continue to operate for at least 72 hours following an outage.

[4] https://phoenixnap.com/blog/data-center-tiers-classification

6. Ensure that the selected CSP adheres to the data protection and security guidelines of the Government[5].

7. Ensure that the selected CSP provides assurance on the following.

    a. All services would be provided in a timely manner, in compliance with best practices.

    b. The CSP would provide a user guide/specification manual to the government organization on the use of the cloud services

    c. The cloud services would comply with legal and legislative principles, rules and regulations in effect in Sri Lanka.

    d. Data and information of the government organizations will not be shared with or disclosed in any manner to a third party by the CSP without prior written consent of the government organizations.

    e. The cloud services would not infringe the intellectual property rights of any third party.

    f. There is no pending litigation involving the CSP that may impair or interfere with the government organization's right to use the solution.

    g. The CSP has sufficient authority to enter into an agreement and grant the rights provided in the agreement to the government organization.

8. Validate and ensure the CSP's ability to perform the following to facilitate data recovery in a situation of emergency or disaster, as per the application criticality and service requirement.

    a. Ensure that it can make the services available even in the event of a disaster, power outage or similarly significant event.

    b. Maintain and implement disaster recovery and avoidance procedures to ensure that no solution is interrupted during any disaster. The CSP shall provide the government organization with a copy of its current disaster recovery plan and all updates thereto during the term.

    c. No government data loss occurs in the absence of data recovery mechanisms.

9. Ensure that the failure of one component of cloud services has less impact on overall service availability and reduces the risk of downtime.

[5] Refer Annex 6 – Data Protection and Security Guidelines

10. Ensure that the disaster recovery solution is owned and managed entirely by the contracted CSP.

1.4 Implement

This stage involves preparing the cloud environment on the CSP platform, installing and configuring the applications, strengthening the production environment, executing testing, final migration and go-live to production cloud. The goal is to ensure all activities are performed in a sequential manner, while minimizing downtime and disruption to services/users.

Government organizations are expected to comply with the following guidelines during this phase.

1. Select any of the following cloud deployment models, in accordance with the organizational requirements.

a. Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It is owned, managed, and operated by a third-party CSP, which exists on the premises of the cloud provider. Users can access the services and manage their account via a web browser.

b. Private Cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers such as business units. It may be owned, managed, and operated by the organization, a third party, or a combination of both parties, and it may exist on or off premises. A private cloud is one in which the services and infrastructure are maintained on a private network.

c. Hybrid Cloud

The cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by technology that enables data and application portability. A hybrid cloud provides greater flexibility, more deployment options, and helps to optimize existing infrastructure, security, and compliance

d. Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns such as mission, security requirements, policy, and compliance considerations etc. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination of them, and it may exist on or off premises.

1.5 Management and Monitoring

This stage enables the Government organizations in adopting a monitoring approach during pre and post migration with the objective to track progress of the ongoing migration of different workloads of the organization and post migration performance indicating any operational, performance issues.

Government organizations are expected to adhere to the following guidelines during this stage.

1.5.1 Pre-Migration

1. Government organizations should analyze their services, needs, technical requirements, and policy constraints in order to prepare for the migration to cloud environment.

2. Data has to be categorized by its sensitivity prior to moving to the cloud. Accordingly, Government organizations should prepare a list of all on-premises systems, applications and software and assign a priority level for migration.

3. Government organizations should carefully analyze their IT portfolio and create a roadmap for cloud deployment and migration. The roadmap should prioritize services that have high expected value and high readiness to maximize the benefits received and minimize the risk.

4. A comprehensive set of test scenarios should be prepared for every system, application, software and process in the on-premises environment to monitor, ensure and confirm the success of the migration and operational efficiency in the cloud environment. The administrators of every system, software, application and process should take the lead in this task.

5. Government organizations should carefully examine and map all of the dependencies in the on-premises solution and make sure that same is retained or improved in the cloud environment.

1.5.2 Migration of the Application / Data (As per the Plan)

1. The on-premises solutions should also run in parallel during the migration process, as a contingency plan, in order to avoid any impact to data.
2. Migration can take a piecemeal approach, where less sensitive data and on-premises solutions must be the initial focus, followed by others based on sensitivity.

3. Government organizations should ensure proper monitoring and validation during the migration process, in order to ensure the successful data migration to the cloud.

1.5.3 Post-Migration

1. Conduct a post-migration validation, using the developed test scenarios, for each and every system, software, application and process in order to ensure that they are producing the same outcomes without disrupting normal operations.
2. Operational manuals, SLAs, governance structures, responsibility matrixes, and support and maintenance contracts should be updated accordingly in order to incorporate cloud migration related updates.
3. CDIO of each Government organization should approve the migration plan confirming that all processes are fully migrated without any impact to data and services and tested to ensure the functionality.

   Note: The availability of a duly approved cloud migration plan is a responsibility of the CDIO.

4. Government organizations should conduct a periodic monitoring and evaluation exercise in order to analyze the following.
   a. Existence of security vulnerabilities which would threaten the confidentiality of data and performance of the applications hosted in the cloud.
   b. Unauthorized deletion and modification of applications and data hosted in the cloud.
   c. User experience in using cloud based applications. Monitor metrics such as response times and frequency of use to get the complete picture of performance.
   d. Monitor and troubleshoot of infrastructure
   e. Analyze the operational logs and metrics in near real time to identify trends and patterns in application performance and use the observations to reduce the mean time to repair (MTTR).