INFOLEX
NEWSALERT

MAY 2017

CLOUD SERVICES: GUIDELINES FOR GOVERNMENT PROCUREMENT

1. INTRODUCTION

The Ministry of Electronics and Information Technology, Government of India (the "**Ministry**") has announced the "*MeghRaj Policy*" (the "**Policy**") providing directions for adoption of cloud services by various government departments (including central, states and municipalities). The Policy comprises the objectives and aims of the Government of India towards procuring and leveraging cloud services offered by cloud service providers.

2. BACKGROUND

The Policy aims to realize a comprehensive vision of a government cloud (GI Cloud) environment available for use by central and state government departments, districts and municipalities to accelerate their information and communication technology enabled service improvements. The Policy stipulates the approach of the Government towards provisional empanelment of cloud service offerings by service providers that can be leveraged by end-user departments in addition to the national cloud services offered by the National Information Center.

3. CLOUD PROCUREMENT

3.1 Key Considerations

The Government has directed that departments should be aware of the following key considerations while making requests for proposal ("**RFP**"):

(a) **Cloud service requirement**

An estimation of the requirements for virtual machines, storage and other information technology platforms for different environments such as pre-production (development, testing), production and disaster recovery.

(b) **Security-shared responsibility**

Consideration of the degree of shared control and responsibility for the cloud environment.

(c) **Operation and maintenance requirements**

Consideration of managed services available for operating and maintaining cloud services.

(d) **Exit management**

The RFP must expressly delineate the responsibility of the cloud service provider during the exit management period and the transitioning of services.

(e) Role of departments during operation phase

Consideration of the role of departments, *inter alia*, in reviewing, validating and auditing security configurations created by managed service providers and the review of released notifications and patches.

(f) Managed services

Consideration of the specific responsibilities of the vendor towards the provision of cloud services, managed services-migration, back up, disaster recovery, operations and maintenance.

(g) *Pay-As-You-Go* utility model

Consideration of the transition from the traditional *fixed payment model* to *variable pricing* where the department pays for the resources it actually uses.

(h) Evaluation of cloud service providers

The RFP should set out either a *lowest commercial quote* (L1) or a *quality and cost based selection* (QCBS) method for selecting cloud service providers.

(i) Migration of existing applications

The RFP should also set out key factors to be deliberated while preparing a plan for migration of legacy applications to cloud based services.

3.2 Models of Engaging the Cloud Service Provider

Based on the requirements, any of the following models can be adopted:

(a) procurement directly from the cloud service provider;

(b) procurement through a managed service provider; or

(c) procurement of end-to-end services through a system integrator.

3.3 Contract Terms

The following key issues are identified as cardinal to the contract with cloud service providers:

(a) privacy and security safeguards;

(b) data breaches;

(c) residence of the data in India;

(d) e-discovery;

(e) payment terms;

(f) transition and exit obligations;

(g) performance management;

(h) periodic audit, access and reporting;

(i) dispute resolution; and

(j) compliance with key international standards such as ISO 27001, ISO/IEC 27017:2015, ISO 27018, PCI DSS and other applicable standards.

3.4 Service Level Objectives

The Policy specifies a minimum target service level of 99.5% with respect to up-time of cloud services and the availability of critical services, including, register support requests, the availability of the network and vulnerability corrections. The penalty for non-compliance of the foregoing may vary from 10% to 30% depending on the nature of non-compliance.

IndusLaw View:

The Policy is an offshoot of the *Digital India* vision of the Government of India. The Policy sets out a clear structure for the cloud service provider and government agencies and departments to engage with each other. However, the approach of empaneling non-governmental cloud service providers may differ based on the nature of the government department and the importance and significance of the data. For instance, if procurement is related to the defence sector, it is likely that the procurement policy will be significantly more stringent. Further, the State Governments also have discretion to establish their own guidelines, in addition to the Policy issued by the Ministry.

Authors: Avik Biswas, Namita Viswanath and Sangeet Sindan

May 15, 2017