Sultanate of Oman
Information Technology Authority

e.oman

Cloud Governance Framework

Governance & Standard Division

VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Standards Division	standards@ita.gov.om	2017
Verified by			
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	All concerned government agencies
3.	Online publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	2017	Governance & Standards Division	Creation of document

Contents

Exhibits

1 Overview

This document provides a framework for adoption of cloud computing with its various adoption and service models. It lists certain benefits, challenges and risks in adoption of cloud computing relevant to government agencies of Oman. The framework showcases organisation, technological and environmental guidelines for adoption of cloud for the agencies of Oman. With the adoption of cloud, the agencies of Oman need to be aware of the legal implications and ascertain that the cloud provider is compliant with the mandates, laws and policies of the Sultanate of Oman.

1.1 Purpose

The Oman eGovernance Framework aims to enhance the delivery of Government Services in alignment with the Mission of e.oman. The framework is aimed at putting controls to minimize risks and better delivery of IT initiatives. As part of the e.oman mission this framework aims to outline the guiding principles towards adoption of cloud. This includes process to identify and assess risks, strategies to assist and secure cloud infrastructure and mechanisms to assure that the strategies have been implemented.

a. This framework introduces cloud computing to the various stakeholders within the agencies of Oman and the process for adoption of cloud computing as a service for various agencies of Oman.

b. The framework provides guidance and helps agencies to decide which cloud model is suitable for them based on certain parameters which would help the agencies make a comparison between existing IT and cloud.

c. The framework provides readiness and adoption elements, some of which are true to any program and some are cloud specific. These elements are adopted from the TOE framework. The TOE framework is an organization-level theory that explains that three different elements of a firm's context influence adoption decisions.

1.2 Target Audience

Mentioned below is the list of target audience for the framework for adoption of cloud.

a. Agencies at the Sultanate of Oman, which would consider adoption of cloud computing and would want to understand the benefits, challenges and associated risks of cloud.

b. Whole of government stakeholders, who may not directly benefit from the framework but maybe interested to understand more about cloud.

2 ENVIRONMENTAL FACTORS

Governments throughout the world are promoting services/e-services in the best possible way to perform daily activities especially in government offices that have direct interaction with citizens. With cloud computing there is considerable scope of speeding up the development and roll out of e-Government applications, and enhancing agility in customizing and deploying ICT (Information and Communication Technology) to meet specific business needs, while at the same time increasing government ICT efficiency (through re-use and service scalability).

The objectives for the agencies of Oman in adopting cloud computing strategy is as follows:

a. Optimum utilization of infrastructure

b. Speeding up the development and deployment of applications

c. Easy replication of successful applications across similar agencies to avoid duplication of effort and cost in development of similar applications

d. Availability of certified applications following common standards at one place.

Keeping in mind the objectives of adoption of cloud, the agencies at Oman should be able to realize the business and technology benefits which are mentioned below:

a. Facilitating federation within agencies by leveraging a solution to a broader set of users instead of just serving one agency

b. The standardized practices, regulatory requirements and restrictions can be propagated through the cloud solution to all the agencies while at the same time each agency can still retain its autonomy

c. Have an improved collaboration through the cross-collaborative business solution

d. Increased focus on delivering services without the need to make huge investments in IT

e. Faster time to market to launch new services

f. Reduced operational costs with reduction in costs of hardware, software and licensing

g. Lower development costs from development and hosting of services and new capabilities.

3 PRINCIPLES

Principles for the cloud computing adoption framework form a basis of conduct. The agencies should adopt cloud considering the cloud-first strategy. The cloud-first strategy focuses on reducing the IT costs by leveraging the benefits of using shared infrastructure and services. The agencies will only pay for the resources consumed. Mentioned below are the principles for the adoption of cloud computing for the agencies of Oman.

a. Enablement: The agencies should plan for cloud computing as a strategic enabler, rather than as an outsourcing arrangement or technical platform

b. Cost/Benefit: Agencies should evaluate the benefits of cloud adoption based on a full understanding of the costs of cloud compared with the costs of other technology platform business solutions

c. Enterprise Risk: Agencies should take an enterprise risk management (ERM) perspective to manage the adoption and use of cloud

d. Capability: Agencies adopting the cloud should integrate the full extent of capabilities that cloud providers offer with internal resources to provide a comprehensive technical support and delivery solution

e. Accountability: Agencies should manage accountabilities by clearly defining internal and provider responsibilities

f. Trust: Agencies should make trust an essential part of cloud solutions, and build trust into all business processes that depend on cloud computing.

4 Introduction to Cloud Computing

Cloud computing is a model of accessing services (business/applications) over the Internet which will be hosted either at a third party location (provider) or at the agencies data centre (consolidated). These services (servers, applications, storage, etc.) can be broadly accessed over various channels (workstations, laptops, mobile phones, tablets) from anywhere, made available on-demand. These services are made available from a pool of resources (virtual/physical) which may be used by multiple agencies and can be shrunk or expanded as per requirements. The service is measured which means that the agencies will pay for only the time the resources were utilized.

Cloud computing promotes availability and is described by five essential characteristics, three primary service models and four deployment models. These are described in detail in further sections.

Characteristics	Service Models	Deployment Models
• On-demand self service • Broad network access • Rapid elasticity • Rapid provisioning • Measured service	• Software as a Service (SaaS) • Platform as a Service (PaaS) • Infrastructure as a Service (IaaS)	• Public Cloud • Private Cloud • Hybrid Cloud • Community Cloud

Exhibit 1 - Cloud Computing Model

4.1 Characteristics of Cloud Computing

The five essential characteristics of cloud computing defined by National Institute of Standards and Technology (NIST), differentiate them from traditional IT and are accepted globally. The five characteristics are briefly defined below:

a. On-demand self-service: The agencies can provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with a service provider

b. Broad network access: Any service (business/support/applications) is available over the network and can be accessed by the agencies via mobile phones, tablets, laptops, and workstations

c. Resource pooling: The provider's computing resources will be pooled to serve agencies using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand

d. **Rapid elasticity:** Any service can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the agencies, the capabilities available for provisioning will appear to be unlimited and can be appropriated in any quantity at any time

e. **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and the individual agencies of the utilized service.

Multi-tenancy is another characteristic not widely recognized by NIST, but still accepted globally. It is the use of same resources or application by multiple agencies that may belong to the agencies of Oman or different organisations (both public and private), and is a very important characteristic of public cloud.

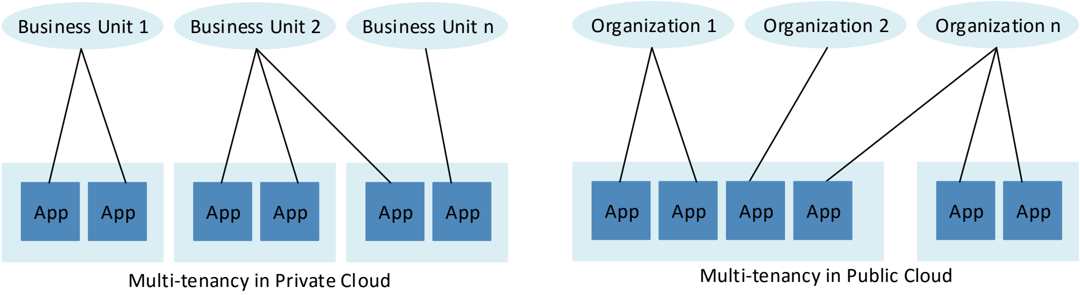


Exhibit 2 - Multi-tenancy in the Cloud

4.2 Adoption Models of Cloud Computing

The first step for the agencies towards adoption of cloud is to choose the delivery model on which services will be offered. The services on cloud can be leveraged by adopting any of the below models:

a. As a public cloud in which a service provider will make services, such as applications and storage, available to the agencies over the Internet on a pay-per usage mode

b. As a private cloud that will be hosted within the data centre of the agencies of Oman; or as a private cloud that will be hosted externally by a third party provider also known as a virtual private cloud. The private cloud will give the agencies to retain the ability to standardize and implement its own best practices

c. As a hybrid cloud, which is a combination of private and public cloud.

d. As a community cloud, where the cloud infrastructure will be shared by several government organisations of the same domain (e.g. governments, dependent agencies, etc.).

The exhibit below highlights the various cloud adoption and deployment models.

Cloud Model	Infrastructure owned by	Infrastructure managed by	Location	Consumed by
Public	Cloud service provider	Cloud service provider	Cloud service provider	Multiple organisations
Private	Agencies	Agencies	Agencies owned data centre	Agencies
Virtual Private Cloud	Cloud service provider	Cloud service Provider	Cloud service provider	Agencies
Hybrid	Both	Both	Both	Agencies, private entities
Community	Cloud service provider or agencies	Cloud service provider or agencies	Cloud service provider or agencies	Agencies, connected third parties

Exhibit 3 - Adoption Models of Cloud

4.3 SERVICE MODELS OF CLOUD COMPUTING

The second step for the agencies towards adopting the cloud is to select the service type.

a. Software as a Service (SaaS)

b. Platform as a Service (PaaS)

c. Infrastructure as a Service (IaaS).

Each service is built on top of the underlying cloud service model and requires the structure and standards of the services below it.

The Exhibit below shows the three cloud service models and what layers form a particular model. The exhibit also shows who (provider / agencies) will manage what within a service model and at the same time compares the models with an on-premises traditional IT model.

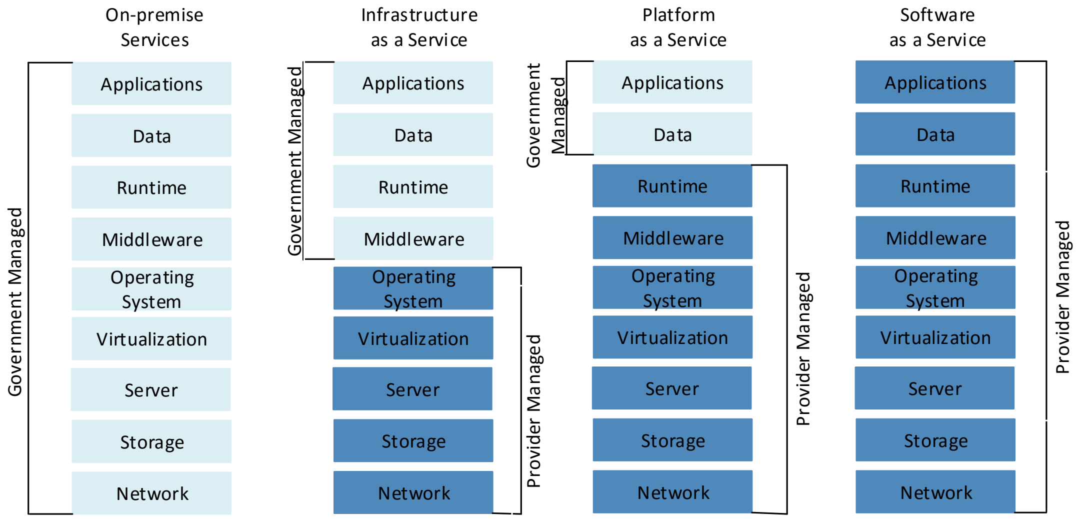


Exhibit 4 - Cloud Computing Models

a. With **SaaS** the underlying infrastructure and platforms are provided and managed by the service provider. The provider will take care of all the software development, maintenance and upgrades. The agencies when opting for such a service will only have to pay for the number of licenses of a software on a subscription basis. Examples of SaaS are Office 365, CRM, ERP, GoToMeeting, etc.

b. **PaaS** is one level higher than IaaS which is ideal for the agencies to build applications and services over the internet with a set of tools supplied by the provider. Agencies can choose from the tools to create applications suitable for their requirement. The underlying infrastructure and the applications will be supported by the provider for the agencies. Examples are virtualization platforms, Java, MySQL services, etc.

c. For **IaaS,** the underlying infrastructure for building, or deploying any services is supplied by the provider. The agencies need to take care of the middleware, operating systems and associated licenses to build those services. Examples are Amazon Elastic Computing (AWS EC2), Rackspace dedicated storage (DAS, SAN, NAS solutions).

From the three major service models there are certain derived cloud service models which are also solutions based on the above three service models. Mentioned below are the examples of the above cloud models.

a. With Business Process as a Service (**BPaaS)** the agencies can adopt applications used for business services such as unified contact centre, time card management, which can be offered built on SaaS

b. Disaster Recovery as a Service **(DRaaS)** is a solution where the agencies can opt for replication and hosting of services off-site (after an assessment or depending on criticality and classification of data) and within the cloud to provide a failover in the event of a man-made or natural catastrophe

c. Security as a Service **(SECaaS)** is a solution to provide secure systems and data in the cloud as well as in traditional IT setup over the Internet. The cloud service provider will offer the agencies services like anti-virus, Identity and Access Management (IDAM) as applications in the cloud

d. Desktop as a Service **(DaaS)** is the provisioning of the backend of a virtual desktop. The cloud service provider will manage the storage, backup, security and upgrades. While the provider handles all the back-end infrastructure costs and maintenance, agencies will have to manage their own desktop images, applications and security.

4.4 FACTORS FOR ADOPTING A CLOUD MODEL

Before the agencies consider adopting a cloud model they will need to evaluate their requirements to understand why a particular cloud model will be suitable for them.

For agencies opting to choose SaaS delivery model for cloud they should take the following into consideration:

a. Agencies should choose SaaS when they want to improve the efficiency of their business related processes by being able to concentrate more on business related processes rather than processes for adoption of a software or technology, and improve the collaboration of a number of different e-services being offered

b. The agencies should know what exactly they want from their SaaS software services and what features the software services will need to have. For example, if the agencies want to improve collaboration between employees to reduce the time taken for an e-service then the agencies can opt for collaboration software as a service wherein employees would be on a single collaboration platform, communicate real-time and resolve any issues effectively and efficiently

c. Agencies should take into consideration the service level agreement which should clearly define what the SaaS provider will offer and also what consequences will they face if they fail to provide these services to the agreed standards

d. With SaaS the agencies will pay lower cost on the hardware and software. For example, if the agency chooses office 365 as solution in the cloud assuming that an agency has only 100 users. The agency will only pay for the 100 user licenses for an active office 365 service in the cloud, the cost for maintenance of the environment will be split between agencies

e. The service provider will be responsible to provide any software upgrades, security patches and the agencies will no longer need to bear costs for upgrades, reduced dependencies on technical staff to test and validate the upgrades, patches.

PaaS as a model will be helpful for agencies if the agencies are planning to develop and deploy applications and services for cloud applications. The agencies should consider the following before choosing PaaS as a delivery model:

a. The PaaS selection model for the agencies should depend on the application and business strategy. For example some PaaS providers offer integration with tools. High level of integration can help reduce the time for deploying applications. The agencies should also consider how an application in the PaaS environment will integrate with other applications and can share data

b. PaaS for the agencies should provide application development, database, integration, and support and security services. Agencies should decide the need for each application in each of the mentioned services. For example if any needs redundant storage then private cloud services might be a better choice

c. The agencies will have to decide on the type of PaaS (portable or vertically integrated) to choose from. The best options for the agencies would be to choose the open source PaaS platforms. Example of open source platforms are Cloud Foundry, OpenShift, Stackato, etc. Vertically integrated platforms seamlessly combine IaaS and Paas offerings and are not portable. These offerings can be found out typically on Azure and AWS platforms

d. The development frameworks and languages which will be supported on PaaS. It is important for the agencies to check and determine the development languages and frameworks supported on PaaS

e. Cost is another factor which the agencies should consider as with PaaS the agencies will need to bear the costs of developing and maintaining the applications will be the responsibility of the agencies.

IaaS for the agencies will be ideal in delivering services on demand where network, storage and servers are available to use. The agencies should consider the following before choosing IaaS as a delivery model.

a. IaaS will be ideal for agencies which have the need for running heavy workloads and at the same time scale resources up or down, quickly and regularly

b. Infrastructure and data security offered by the provider meets and exceeds the standards of the agencies

c. With IaaS, the agencies can adopt a consolidated DR infrastructure with reduced costs resulting in quick recovery without any loss of data

d. For agencies the cost of maintaining or replacing equipment are lower. Agencies no longer will need to worry about uptime as it will be the provider responsible to maintain the uptime in case of upgrades and maintenance cycles.

The agencies should perform a cloud affinity assessment which should involve evaluating the information form against the drivers and inhibitors of cloud adoption and determine the viability of a cloud service.

Parameters	Cloud adoption inhibitors				Cloud adoption drivers		
	-3	-2	-1	0	1	2	3
Scalability							
Elasticity							
Adaptability							

Parameters	Cloud adoption inhibitors				Cloud adoption drivers		
	-3	-2	-1	0	1	2	3
Financial Strategy							
Skills							
Security							
Integration effort							
Exit strategy							
Urgency							
Project Duration							

Exhibit 5 - Cloud Affinity Assessment

The above exhibit shows a scale from -3 to 3 ranging from strong inhibitors to strong drivers. If inhibitor weighting scores higher than driver weighting, then the agencies should consider avoiding certain cloud adoption patterns. For example, it is better to store and use sensitive data on a private cloud. If the opposite is true and the driver weighting scores higher, then the cloud decision process should proceed with a broader range of potential adoption patterns.

The agencies must use a solution score metric to evaluate different services and applications for adoption and to choose which cloud model will be better suited for the applications and services.

Score	0=Poor	1=Average	2=Good	3=Excellent
Fulfilment of the requirements	Not fulfilled	Partially fulfilled	Completely fulfilled	Overachieved
Trade-off	Selecting this service/app leads to a major compromise	Selecting this service/app leads to a trade-off	There is no trade-off with selecting this service/app	There is no trade-off with selecting this service/app

Exhibit 6 - Solution Score Metrics

5 VALUE PROPOSITION AND RISKS

This section presents certain benefits, challenges and risks towards adoption of cloud computing as a service. Cloud computing eliminates the need for heavy infrastructure investments and offers flexible operating models. This will help the agencies of Oman to enhance business agility and market responsiveness. As cloud offers certain benefits there are also associated challenges and risks which are highlighted in the below sections.

5.1 VALUE PROPOSITION

Below are a few compelling features that will make the cloud model attractive to agencies of Oman:

a. Flexibility: Cloud-based services are ideal for agencies, which have fluctuating IT requirements. Whenever there is a need to scale up or down any service it can be flexibly tuned as per the requirements. This level of agility can give agencies using cloud computing a real advantage to bring up new services in a quick span of time

b. CapEx reduction: Cloud computing cuts out the high cost of hardware. The agencies only pay for the utilized resources and services with the ease of tuning/scaling up servers and services within minutes

c. Asset utilization: Cloud computing will promote highly efficient IT asset utilization for the agencies. It will help reduce considerable duplication of equipment and effort across agencies and departments. When they can share applications, storage, and compute power, the agencies will not have to build for peak usage

d. Disaster recovery (DR): As the agencies have to process and deal with a lot of public data which maybe classified and confidential, setting up a DR is of utmost importance. For smaller agencies that lack the required funds, resources and expertise a DR solution in the cloud is more ideal than the reality. The turnaround will be quick avoiding large upfront investments with provider support available round the clock

e. Improved Performance: A high performing cloud platform can support resource intensive applications and also help achieve Service Level Agreements (SLAs) for the agencies within Oman

   i. With faster processing, agencies can run critical applications in the cloud more cost effectively and reliably with savings on CapEx and OpEx and at the same time avoid duplication of assets and improve asset utilization.

   ii. Big data, analytics, modelling and simulation can run more efficiently due to faster disk access, memory, and throughput.

a. Automation: Automation will enable agencies to self-provision resources (CPU, RAM, disk space, etc.) on a server which can help agencies run services efficiently with required performance and without any intervention

b. Improved collaboration: All documents can be centrally stored at one location and every agency will be able to work and update documents simultaneously. Cloud will allows employees dispersed to meet virtually and easily share information in real-time leading to improved collaboration

This document provides a framework for cloud computing adoption with its benefits, challenges and risks. For any information on collaboration services, it is to be referred to the Technical Reference Model.

c. Service and resource upgrades: The agencies do not need to worry about applying security patches or application upgrades needed to run the business. Upgrades and patches are tested and made available to agencies by the provider after tests

d. Green IT: With cloud computing, agencies can reduce the size of their own data centres - or eliminate their data centre footprint altogether. The reduction of the numbers of servers, the software cost, and the number of maintenance staff can significantly reduce IT costs without impacting the IT capabilities

This document provides a framework for cloud computing adoption with its benefits, challenges and risks. For any reference on standards and best practices on Green IT, refer to the Technical Reference Model.

5.2 Challenges

Business and IT stakeholders perceive that agencies are most concerned about security, difficulty measuring Return on Investment (ROI) and determining the accurate economic value of the solution followed by governance of cloud-based services with respect to government and global standards.

Listed below are typical challenges from a government organisation perspective including concerns about security, integration challenges and information governance

a. Service quality: Service Level Agreements (SLAs) by the providers are not stringent and adequate to assure that the services will run with the desired level of availability, performance and reliability. There are certain aspects which the agencies should keep in mind and the cloud provider should be able to answer with regards to service quality such as:

i. The minimum service levels desired by an agency

ii. The remedies which are in place when a failure occurs

iii. The disaster recovery and business continuity procedures

iv. Portability of the agency data

v. The change management process which the provider follows

vi. Infrastructure and security standards of the provider

vii. Time taken by the provider to identify and isolate problems

viii. Escalation process with the cloud provider

ix. Exit strategy with the provider including roles and responsibilities

x. The process of contract termination with the provider.

b. Vendor Lock-in: Cloud service providers will assure the agencies about their cloud being flexible to use and can easily be integrated with other providers or with in-house service capabilities, however switching providers hasn’t completely evolved. Agencies may find it difficult to migrate services from one vendor to another due to interoperability and support issues between providers

c. Downtime and Accessibility: The agencies will have to access the services and their data via an internet connection rather than a local connection. So when the network or internet connection is down, it will also mean that cloud services will be down. Performance of the cloud infrastructure can be affected by the load, environment and number of users. Ensuring that the cloud infrastructure is resilient to outages is vital for the agencies. While it will be almost impossible to mitigate all outages, a provider with robust and resilient measures should be chosen to protect government data

d. Network dependencies: If the agencies decides to opt for a hybrid cloud integration model network dependencies will require thoughtful design involving the below parameters:

   i. Impact of latency (also known as time delay) between the private cloud and public cloud infrastructure

   ii. Identifying bandwidth hungry applications that will struggle to work over wide area networks

   iii. Bandwidth for transferring large data sets

   iv. Using the existing IP blocks in a hybrid topology and usage of IPv6 if and when required

   v. Using the security appliances and solutions being used in the traditional IT / private cloud onto the public cloud.

This document provides a framework for cloud computing adoption with its benefits, challenges and risks. For any reference on network dependencies, policies are to be referred to in the Technical Reference Model

e. Transition to the cloud: Transitioning to the cloud is a complex and involved process, the agencies must ensure that the proposed solution compliments their business model. There are certain aspects which the agencies should keep in mind that a cloud provider would want to know:

   i. The demand patterns of services for agencies

   ii. Biggest influx of data for any agency

   iii. Year on Year data growth for the agencies

   iv. Constraints for agencies with the location of data

   v. Control over data required by the agencies

   vi. SLA expectations of the agencies.

f. **System Management:** Lifecycle management of hybrid cloud systems can be a challenge if done incorrectly and the agencies needs to be thoroughly prepared to understand and achieve the below:

   i. Effective configuration management when infrastructure resources are provisioned in self-service across environments

   ii. Achieving security and patching of multiple environments

   iii. The nature of capacity planning changes when dealing with elastic resource pools

   iv. Achieving Integrated and effective monitoring in the hybrid cloud.

This document provides a framework for cloud computing adoption with its benefits, challenges and risks. For any reference on network dependencies, policies are to be referred to in the **Technical Reference Model.**

5.3 RISKS

With every adoption of technology are certain impediments which may rise from known and unknown factors. Mentioned below are risks which are associated with the adoption of cloud.

a. **Security and Privacy:** Data and information security in the cloud is usually at optimum levels, and generally reliable and proficient. Both the public and private cloud providers are compliant to various standards, however agencies maybe more reluctant to hand over important data to a third party provider as they deal with restricted and confidential data, and data in the cloud could be stored and backed-up anywhere across the globe. A few security aspects which need to be considered by the agencies are:

   i. Data location in the cloud

   ii. Security and encryption of data

   iii. Security and governance policies of the cloud provider

   iv. The control the agencies will have over its data and environment

   v. Time taken to backup an agency data in the cloud

   vi. Data audit procedures of the provider

   vii. Data recovery in case of data corruption

   viii. Data extraction procedures for the agencies if the service needs to be moved in-house or to any other cloud provider.

While this document provides guidelines towards adoption of cloud with associated benefits, challenges and risks, any policies on information and its security are to be referred to the **information security management**

b. **Limited Control:** In public clouds since the cloud infrastructure is entirely owned, managed and monitored by the service provider, it may transfer minimal control over to the agencies. The agencies can only control and manage the applications, data and services operated on top of that, not the backend infrastructure itself. The agencies will have to agree with the governance, compliance and management policies of the provider.

While this document provides guidelines towards adoption of cloud with associated benefits, challenges and risks, any policies on information and its security are to be referred to the **information security management**

c. **Location of data:** Cloud computing is a borderless concept and with most providers data or a copy of the data is stored at a different geographic location other than the base location to recover from a breech or a catastrophe. At Oman the agencies need to consider the following:

   i. Conditions Relate to data ownership, accessibility, privacy and security

   ii. Decision regarding storage and transmission of data to different cloud model.

   iii. Application sensitivity, data classification and other relevant privacy and security

   iv. Regulatory and legal framework of the hosting jurisdiction.

While this document provides guidelines towards adoption of cloud with associated benefits, challenges and risks, any policies on information and its security are to be referred to the **information security management**.

d. **Interoperability and Compatibility:** If any agency decides to move to a different cloud provider or maybe in-house there might be possibilities that the different solutions are running different infrastructure and software stacks. This poses a risk in considering whether the same change management processes be used across the hybrid cloud, or are each unique depending on the provider.

e. **Legal regulations:** For agencies compliance with regulatory and legal standards are very important. The cloud provider and agencies are responsible to abide to legal regulations. Whenever any agency adopts and deploys a cloud model there are some issues which the agency should consider at all stages of the contractual process which are as follows.

   i. Initial due diligence

   ii. Contract negotiation

   iii. Implementation

   iv. Termination (end of term or abnormal)

   v. Supplier transfer.

While this document provides guidelines towards adoption of cloud with associated benefits, challenges and risks, any policies on information and its security are to be referred to the **information security management**.

5.4 Comparison of Traditional IT with Cloud

Adopting cloud has its own benefits when compared to traditional data centre approach. Agencies may evaluate the benefits of adopting cloud over a traditional approach by carrying out feasibility assessments, cost benefit analysis, etc. The agencies need to consider the below:

a. Owning a data centre will have huge upfront investments and will require skilled manpower to manage and maintain the services hosted

b. Other than the data centre rack and stack there is a requirement for power to keep the services up and running with a backup system in place via an alternate source

c. Efficient cooling to keep the infrastructure up and running without hot-spots, and requirements of wiring closets

d. Always a demand for more space with ever increasing need and demand for services

e. Additionally the agencies will have to procure the network, server and storage infrastructure and keep them up to date with latest upgrades and patches, employ/outsource management and maintenance staff. Further, buying and building up services will require licensing costs depending upon the number of users and this cost keeps on increasing with an increase in the number of users and service capabilities. There will be costs associated with monitoring and management tools with the requirement of skilled staff to monitor and manage the availability of the services as per the RTO and RPO needs

f. IT refresh will be another big exercise which the agencies will have to follow over a period of time as the solutions, services and products will be at end of life and OEM's will stop releasing upgrades and security patches.

The exhibit below provides a comparison of Traditional IT with cloud as a service model.

Parameter	Explanation	Traditional	Cloud
IT Monitoring / Management Efforts	Refers to the level of automation for monitoring of equipment's	High manual effort despite tools	Significantly reduced due to cloud management / monitoring tools. Enables faster ROI; Reduced Operational expenditure(OpEx)
CapEx	One time cost required to setup the data centre and IT infrastructure	Dedicated infrastructure highest cost	Capex needed to build enterprise cloud. Chargeback based on monitored usage of compute/storage/network Apps show ROI faster; Cloud investment recovery via chargeback
OpEx	Refers to the operational expenditures required over a period of time, maybe over a	Higher due to no. of FTEs, power, cooling, etc.	Reduced when compared with traditional IT due to virtualization and automation; VMs are vanilla and service restoration is via redeploy of O/S, Easier

Parameter	Explanation	Traditional	Cloud
	period of 3-5 years		management of assets; Reduced OpEx;
Utilization	Utilization refers to the amount of IT resources which are being consumed at any point of time	Typically 5-20%	Optimized (60-70% is typical). Can redeploy resources from other pool types, reducing overall infrastructure requirement. Reduced OpEx, quicker TTM, greater agility
Availability	Availability is the desired uptime of equipment and services as per agreements	Clustering can provide 99.9% but at 2 x cost	Suitable applications scale horizontally with re-startable transactions meaning 0 downtime Quicker turnaround; Reduced OpEx
Elasticity	Degree to which capacity of the system can be increased or decreased as required	Scaling up / down is a planned exercise based on procure	Scaling up / down is automatic on-demand and theoretically infinite surges in need are serviced on-demand by cloud (cloud bursts)
Scalability	Ability of a system to increase the workload on its current hardware resources	Peak load sizing at outset. Resizing cumbersome	On-demand automatic scaling as hardware in cloud pool allocated on demand Reduced OpEx; Capacity planning for average loads reduces CapEx

Exhibit 7 - Comparison of Traditional IT with Cloud

5.5 Stakeholders, Roles and Responsibilities

To adopt the cloud computing adoption framework and to provide future guidance within the agencies stakeholders will have a role from a business, technology or process perspective in guiding agencies towards adopting this framework.

The Head of IT of agencies will be responsible however not limited to the below:

a. Strategic review of the framework in-line with the various stakeholders needs within the agencies and keeping it aligned with the key missions of the agencies

b. Work with the sponsors to manage the budget and associated funds, review the same at appropriate intervals

c. Oversee the adoption of the framework with associated challenges and risks and inputs from stakeholders

The IT architects of the agencies will be responsible to the below:

a. Assess the maturity of existing IT including data centre, applications and technology

b. Define the governance model for the adoption of cloud and to ensure compliance with standards and regulations

c. Formulate a plan for adoption of cloud computing.

5.6 Legal Implications for Adoption of Cloud

The agencies of Oman and the cloud providers have to abide by laws, regulations and mandates to protect data and the security of information. The agencies have to make sure that the cloud providers have adopted reasonable technical, physical and administrative measures in order to protect agencies data from loss, misuse or any alteration.

Some of the key privacy and data protection considerations in a cloud computing environment are:

a. The agencies of Oman will have its own data security and access management policies. The cloud provider's policies should be compliant with the policies of the agencies

b. For the agencies of Oman the location of data is of prime importance. At any instance the data or any copy/backup should remain within the legal boundaries of Oman

c. In case of an attack where agency data is lost there should be documented procedures on how provider will recover the lost data

d. Under the Oman jurisdiction the cloud provider will have to abide by different data retention and leakage & data destruction obligations – both online and offline data

e. The cloud provider should not differ and should not change in future any legal and regulatory requirements on data encryption standards to strengthen the security of data residing in the cloud

f. The provider should comply with increased control obligations if at any point of time the laws at Oman are changed

g. If required the provider should be open to share their security policies and at the same time be open for external audits, and share internal audit reports

h. The agencies might require the provider to implement national standards, the details of which may vary insignificantly

i. The provider should specify if the agencies will lose control over the cloud environment and to what extent

j. The provider should be up to date with the change management process of the agencies and if required should update and share the change management process

k. In case of a breach there should be provision for liability towards the provider, proactive response towards the agencies and indemnity by the provider for non-compliance

l. The agencies of Oman might ask the provider to fulfil the conditions for an escrow till the contract is made available on paper

m. The agencies will require alerts (email/SMS/calls) on outages and breaches, service availability reports on monthly basis. In case of a force majeure the cloud provider will try its best to make the services available as soon as possible.

n. The agencies will need to know if the provider has contracted any third-party for service maintenance and support

o. Any agency at any time or at the time of signing of an agreement might want to know the cloud provider staff skill-set and might want to conduct background checks of employees at providers who support the agencies

p. The agencies should be aware if the cloud provider has the ability to change the terms of the contract, the fees and rate structure without advance notice

q. The agencies should know the clear description of the cloud service which should include the type of service provided, the functionalities and whether or not the services will evolve during the contract. This will help the agencies define SLAs

r. The agencies will want to limit access and use of their data by the cloud provider and associated third-party unless and until a proper approval process is in place

s. The agencies should be informed in advance before expiry of a contract and conditions under which the contract may be terminated or extended

t. In case of termination of a contract the agency deserves the right to know what will happen to the data. How can the agency retrieve the data, and in which form and format. During a transition period the provider should be supportive to keep the data for a required period of time.

6 GUIDELINES FOR CLOUD READINESS AND ADOPTION

Cloud computing paradigm shift in service delivery where hosted services are offered through the internet with business innovation and cost benefits. Cloud computing will help the agencies improve business flexibility despite the back-end silos. Agencies will be able to support their mission-critical operations with agile and innovative cloud deployments that enable the use of social, mobile and analytics technologies with stringent compliance and security measures to not compromise on data security.

Some of the key areas on which the agencies will be able to focus with adoption of cloud are:

a. IT Consolidation

b. Shared Services

c. Citizen Services.

Consolidation of IT will involve centralization of multiple scattered data centres of various agencies. Each data centre will have to be assessed for cost, applications and server consolidation and virtualization of services.

The agencies will have services, applications, databases, gateways, etc. which might be common across departments. Shared services will support the agencies to reduce financial uncertainties, and offer money-saving economies of scale and opportunities for rolling out new services more quickly for employee's citizens and businesses.

Citizen services like storage space for digitized documents, online attestation services, birth registrations, etc. could be offered on the cloud. A new server offering these services could be setup within minutes in the cloud without any manual intervention.

The agencies will have to identify and classify applications as below to be suitable candidates for adoption of cloud:

a. Common: Applications which are common across all agencies such as portals, human resource management, repositories, etc

b. Group: Applications such as education, health management, IT requirements management can be suitable candidates to be called as group applications and adopt cloud

c. Department: application which may be common across a few departments can be generalized and be suitable for adoption of cloud such as police, prosecution, municipalities, etc.

The guidelines for adoption of cloud are based on the Technological, Organizational and Environmental (TOE) context which describes factors that influence technology adoption and its likelihood.

6.1 GUIDELINES FOR READINESS

Adoption of cloud is a radical shift from the way technology is being used and will require support and readiness from the highest level of stakeholders being informed and creating a business case and finding a sponsor. The key elements of readiness at different stages of adoption are mentioned below.

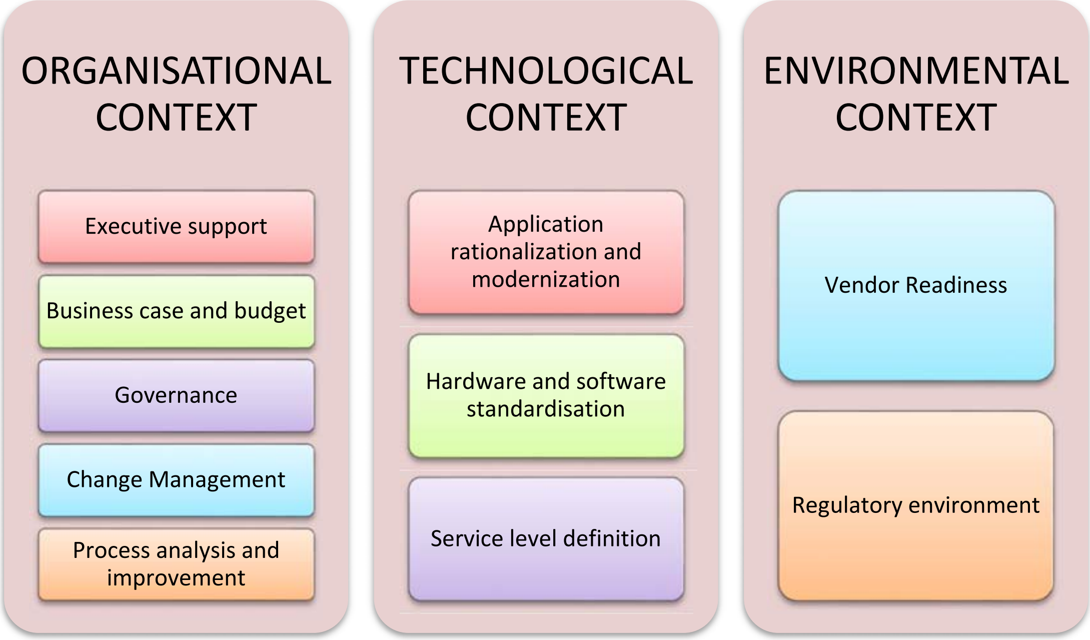


Exhibit 8 - Elements of Cloud Readiness

6.1.1 Organisational Context

From an organisation perspective the agencies focus on the openness to innovation and processes that accommodate change as being essential factors for adoption of cloud.

a. Executive support: For successful adoption of cloud, agencies of Oman will need deep involvement of business functions and overhaul of existing technology landscape. This would necessitate executive support at various levels within and between the agencies to create objectives of the program, keep up with the adoption plan, and to provide oversight at a sustained level

b. Business case and budget: The adoption of cloud will be associated with multiple other programs and steps which would require building a business case. The business objectives for all the agencies should be clearly articulated with the desired future and necessary investments

c. Governance: Governance of the entire cloud adoption and associated programs and steps will be important from the agencies perspective to avoid time and cost overruns. The cloud program will need a combination of business and IT governance for its adoption to be a success. The agencies might need to re-organize their governance organisation for adoption of cloud or build an independent governance team

d. **Change Management:** With adoption of cloud the agencies will have to go through a change within their IT organisation. Depending on the nature of the cloud adoption exercise these changes could be sweeping in nature requiring frequent, multi-faceted and sustained change intervention. The agencies will need to be prepared to go through this cultural shift

e. **Process analysis and improvement:** The IT organisation of the agencies will benefit from the move to the cloud. The biggest benefit will be from opting SaaS as process analysis and improvements will align the business process with the changes to software application and services and in turn enables the business processes to best utilize the capabilities being offered by the applications.

6.1.2 Technological Context

The agencies will need to focus on internal technologies and available cloud technologies and solutions in the market. Internally, adoption of cloud will rely on competent employees who can manage an appropriate technical infrastructure and have e-business know-how. Externally, e-business technology availability is necessary.

a. **Application rationalization and modernization:** For the agencies, a move to the cloud would allow them to evaluate their application landscape, understand the usefulness of the applications and perform a clean-up. Application portfolio modernization is an important aspect of moving to the cloud as it will help rationalize the portfolio and avoid having two environments – the cloud and the legacy environment. Maintaining these two environments will prove costly. For any agency the modernization and move to the cloud should be as per the expected agency standards

b. **Hardware and software standardisation:** For any agency to adopt cloud computing, the first step would be to consolidate their infrastructure, platforms and software. Each agency would then need to develop their standards. For adoption of cloud, every agency would need standards which would be driven from architecture group initiatives which themselves would undergo transformation throughout the cloud adoption journey. Till the time standardization is not overdone every agency will be able to drive flexibility and agility. Hardware and software standardization would be a critical driver for most of the cloud benefits and every agency would require to achieve a balance between today's priorities and future aspirations.

This document provides a framework for cloud computing adoption with its benefits, challenges and risks. For any reference on hardware and software standards, refer to the **Technical Reference Model**

c. **Service level definition:** The technology requirements for the agencies will be delivered as services in the cloud. The service levels will define what is that the agency desires from the service. For the IT organisation at the agencies it will serve as a measure against Key Performance Indicators (KPIs).

6.1.3 Environmental Context

The environmental context includes readiness of the vendor to offer cloud services, the cloud competitors in the market, the macroeconomic context, and the regulatory environment.

a. **Vendor Readiness:** Any agency which wants to adopt a cloud model will have to consider the readiness of vendors which may or may not be part of their historical consideration. The agency will also need to consider solutions which are open source standards. Vendor readiness will effect cloud adoption to a great extent and when switching cloud providers

b. **Regulatory environment:** The regulatory environment can both promote and slow cloud adoption and transformation. Government and global regulations can force resources to be allocated for compliance.

6.2 Guidelines for Adoption

For the Oman agencies looking to adopt cloud or in the process of adopting cloud, the journey to cloud will have certain milestones. Any agency which will adopt cloud will have to go through one of the phases of the milestones. These milestones are progressive in nature, with one leading to another and the eventual state is a hosted cloud solution. These milestones will certainly vary with how agencies will define their cloud programs.

6.2.1 Organisational Context

a. **RFP and tendering process:** Depending upon the size of the agency – a large agency usually will go through an RFP process to articulate the agency objectives and requirements for external partners and identify organisations to provide consulting on cloud, implementation and sustenance in the cloud. The RFP process will be a learning opportunity for both the external partners and the agency and will help define the service level definitions and overall expectations from the cloud adoption program.

6.2.2 Technological Context

a. **Proof of concept:** The proof of concept will help realize the cloud services which will be adopted and deployed, integration between various layers of cloud and will provide input for selection of technologies. Proof of concept is an important aspect to be considered for any agency as many of the tools used in cloud are based on open source and the IT organisation of the agency might be using the tool for the first time

b. **Vendor selection:** For any agencies the inputs from the RFP and PoC phase will help in identifying partners for cloud implementation. These partners could provide cloud consulting, application rationalization services, infrastructure maintenance, cloud tools and technologies and change management. In this stage the agencies have to firm up on their options of cloud technologies to be deployed and which partner will execute the deployment strategy

c. **Cloud service model:** During this stage of the process various cloud service models will be offered to the agencies. Depending upon the maturity, need for governance and control an agency may choose to opt for any of the cloud services model right from IaaS, PaaS & SaaS and any of the built-upon cloud models.

   i. A bigger or more mature agency might choose IaaS as a service to have control, set and deploy its own software standards and scale services as per demand and future requirements

ii. For another agency DaaS might be a suitable model which offers central application of policies and also brings individual change into focus. With Bring Your Own Device (BYOD) trend an employee or user can bring his own device and work on them with full compliance on data privacy and security. For employees who work remotely or travel DaaS might be a good solution as a parallel desktop environment

iii. Similarly any agency who wants to build its own set of services/applications might choose PaaS for development and test environments with availability of development platforms.

d. **Integrated cloud platform:** This is the stage where agencies would have successfully transformed themselves into a state where all infrastructure, platform and software services would be metered, billed and charged to them on a pay-as-you-go basis with boundless scalability.

6.2.3 Environmental Context

a. **Competitive offerings:** Security and legal issues are the major environmental factors which every agency should work with the cloud provider to sort their data jurisdiction, data confidentiality and security risk. With this the agencies will be able to adopt and offer better services to its employees, citizens and business houses. Agencies will be able to utilize SaaS offerings with or without any customization and have more of their employees focus on work.

6.3 Identifying the right cloud model

Every agency will be different with a different set of infrastructure and varying workloads. Demands will also change, so the infrastructure choices the agencies will make will affect the ability to deliver new capabilities. That is why agencies must look for the cloud solution that meets their business requirements in the most effective way. To help the agencies do that, here are five steps for choosing the right cloud solution.

a. Agencies should know their workloads

b. Agencies should collaborate

c. Analyse infrastructure top to bottom

d. Consider process requirements

e. Match and adopt the right cloud solution.

Specified below are category of applications that maybe a good fit for moving to the public cloud:

a. **Dev/test applications:** The largest percentage of compute instances on major cloud providers (like Amazon Web Services) are dev/test workloads. The build and test process tends to be compute-intensive, and therefore a fit for public cloud computing.

For the agencies there will also be less risk to test and develop applications if any as the tests can be done using dummy data

b. Personal productivity applications: Word processing, spreadsheet and presentation design, e-mail software tend to be a good fit. These applications are based on unstructured data and generally don't require low latencies

For the agencies if the data and copy of the data is stored within the jurisdictions of Oman with high level of data security then the agencies can look to opt for a public cloud for such applications

c. Collaborative applications Social networking, web conferencing and other collaborative applications are good for the cloud, especially since many of these solutions were written for the cloud in the first place. For the agencies social such platforms will serve as a way to reach and communicate with the citizens and businesses at Oman. Legacy applications such as SharePoint can also be run in the public cloud

d. High-performance computing (HPC) applications: If the agencies have applications which tend to consume a very high amount of resources (CPU, RAM, Disk Space, etc.) then such applications are usually a good fit for public cloud compute farms, as long as their data needs can be managed.

Applications that are fit for moving to the private cloud:

a. Mission-critical applications: Mission-critical applications such as ERP are transaction-intensive, with high throughput and low latency requirements. For agencies running ERP, they will contain sensitive data and often large datasets, and have high availability requirements. Some such applications may also have regulatory compliance needs that may be difficult to meet in the public cloud

b. Network-intensive applications: Such applications require fast, high-quality network resources that continually transmit and receive large amounts of data. These applications might often require access to, or integration with, other applications to share data.

A technical assessment will be required to understand which applications are more suited to the cloud architecturally and strategically. The agencies will have to determine which applications to move into the cloud first, which applications to move later and if any applications should remain in-house.

During the technical assessment phase, the agencies should find a solution to the below:

a. Which business applications will move to the cloud first?

b. The cloud should provide all of the required infrastructure building blocks

c. Can the agencies reuse existing resource management and configuration tools - if any?

d. Can the agencies get rid of support contracts for hardware, software and network?

The exhibit below shows generalized cloud selection parameters which the agencies can use to select and identify the best suitable candidates for the cloud.

Parameters	Public Cloud	Private Cloud	Hybrid Cloud
Level of Abstraction	High	Low	Moderate
Tenancy	Either a single-tenant (dedicated) or multi-tenant (shared) operating environment	Single-tenant (dedicated) operating environment	A combination of public and private cloud offerings that allow for transitive information exchange
Level of Security	Low. No access to data in provider premise	High. Full access to data is available	High. Full access to data is available
Vendor Lock-in	Depends upon the technology used	High. Depends upon the technology used	Depends upon the technology used
CapEx	Low. As most of the infrastructure is maintained by the provider	High. The in-house infrastructure has to be prepared for deployment	High. It is a combination of public and private cloud
OpEx	High. Continuous pay per usage charging	Moderate. Only one time setup charge is high	Moderate
Managed by	Third party	Agencies or third party	Both agencies and third party
Level of Virtualization	Depends upon the technology used	It provides intelligence over virtualization	Virtualization level is lower than that in private cloud
SLA Guarantee	Difficult to obtain	Easier to obtain and monitor	Easier to obtain and monitor
Suitable for	SMB	Enterprise	Both
Data Privacy	Low	High	Moderate
Legal and compliant issues	High since data may have to be stored on foreign land	Low since data resides in our own data centre	Low since data resides in our own data centre
Types of application Suitable	Less mission critical application having less integration level	Application dealing with highly confidential data	Application dealing with highly confidential data
Infrastructure Owned by	Third party	Organization or third party	Both Organization and Third party

Exhibit 9 - Cloud Deployment Model Selection Parameters

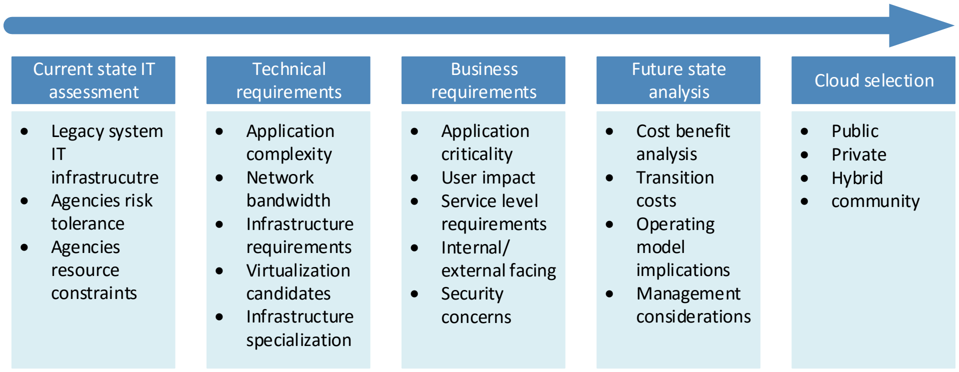
6.4 CLOUD READINESS ASSESSMENT

The assessment phase will include conducting an assessment of the current state, requirements definition, and developing a vision for adoption of cloud. The current state assessment will provide a go no-go report and should be based on the below:

Current state assessment	Requirements definition	Define vision
a. Understand legacy systems – technical and operational environment b. Assess the fit of product offering c. Assess agencies data compliance and security needs d. Assess agencies IT infrastructure for continuity and application interdependencies e. Assess agencies risk tolerance and resource constraints	a. Interview key stakeholders b. Conduct requirement definitions workshop c. Validate requirements document d. Define compliance and security needs for new cloud solution	a. Define goals of the agencies b. Define short term and long term vision c. Define level of migration to the new cloud solution

Exhibit 10 - Cloud Readiness Assessment

The output of the current state assessment for the agencies will be the current state documents, requirements document and a scope & vision statement.



Current state IT assessment
- Legacy system IT infrastrucutre
- Agencies risk tolerance
- Agencies resource constraints

Technical requirements
- Application complexity
- Network bandwidth
- Infrastructure requirements
- Virtualization candidates
- Infrastructure specialization

Business requirements
- Application criticality
- User impact
- Service level requirements
- Internal/ external facing
- Security concerns

Future state analysis
- Cost benefit analysis
- Transition costs
- Operating model implications
- Management considerations

Cloud selection
- Public
- Private
- Hybrid
- community

Exhibit 11 - Assessment Approach

a. Agencies must meet assessment criteria at each step prior to passing on to the next. Agencies should give a score for each criteria (red/yellow/green)

b. Even within each area, failure to meet fundamental evaluation criteria would mean that suitability is no longer viable and the application is not suitable for cloud at this time

c. Agencies applications should exhibit the following attributes and will be assessed accordingly.

   i. Low or moderate application criticality

   ii. Minimal to some interdependencies on other apps / data

   iii. Uses commodity hardware

   iv. Bandwidth requirements

   v. Standalone environments or software stack

   vi. Does not depend on specialized appliances

   vii. Low / moderate SLA requirements

   viii. No confidential data or data can be easily masked.

Phase	Criteria	Explanation
Current State Assessment	Legacy system criticality	Defined by agencies for production environments,
	Legacy system complexity	Architecture complexity, dependencies on other applications, databases, middleware
	Virtualization candidate	Can the workload be virtualized? This depends on the platform OS and virtualization platform
	Commodity infrastructure	Workload runs on commodity infrastructure
Determine Suitability for Cloud	Technical Feasibility	
	Network bandwidth	LAN or WAN network bandwidth requirements when workload would run in the cloud
	Infrastructure requirements	The scale of requirements for compute, storage and network to support workload
	Shared environments	Types that would be supported by a shared environment
	Shared software	Software (e.g., databases, middleware) share with other software

Phase	Criteria	Explanation
	Specialized infrastructure	Dependency on special purpose proprietary appliances, devices, license , hardware, etc.
	Business Feasibility	
	Internal / External Facing	Does the system provide a customer facing service or back office function (e.g., HR)?
	User impact	Impact on the user community due to move of workload to cloud (e.g., lack of access to a subset of users)
	Service level requirements	Availability, response time, Recoverability , Disaster Recovery, etc.
	Customer / Confidential Data	Does the provider location or other characteristics of the cloud service meet the security requirements of how and where data needs be stored?
Business Case and Operational Analysis	Business case analysis	Cost/ benefit analysis, including initial and migration costs, on-going costs and ROI timeframe
	Detailed technical analysis	What changes will be required for the application? What will the future application architecture look like?
	Operational analysis	What is the operational impact due to the workload moving to cloud? What is support model after workload is moved to cloud? What is provider vs. client responsibility and hand-offs?
	Management considerations	How is the workload managed in the cloud? E.g., using internal and vendor provided tools, processes, and staff; Go–No/Go Based on Assessment Scorecard

Exhibit 12 - Assessment Criteria

Based on the assessment and considering the above points the agencies can make a decision whether to adopt cloud or not.

	Red	Yellow	Green	Go/No-Go Decision
Current State Assessment				
Technical Feasibility				
Business Feasibility				
Go/No-Go Decision				

Exhibit 13 - Decision Matrix

a. If the number of "Red" ratings are at the most 1, the agency may decide to "Go" into the cloud solution, else this may be a "No Go"

b. If the number of "Yellow" ratings are at the most 2, the agency may decide to "Go" into the cloud solution, else this may be a "No Go"

c. The number of "Green" ratings should at most be 2 for the agency to decide to "Go" into the cloud solution, else this may be a "No Go".

The Appendix section provides information about the various risk domains which the agencies should be aware of and a risk assessment questionnaire for the cloud.

The section below provides a detailed roadmap which the agencies should consider towards adoption of cloud.

6.5 Roadmap for Cloud Adoption

For the agencies to adopt cloud they will have to go through five phases and twenty one stages which are mentioned in the exhibit on the page below.

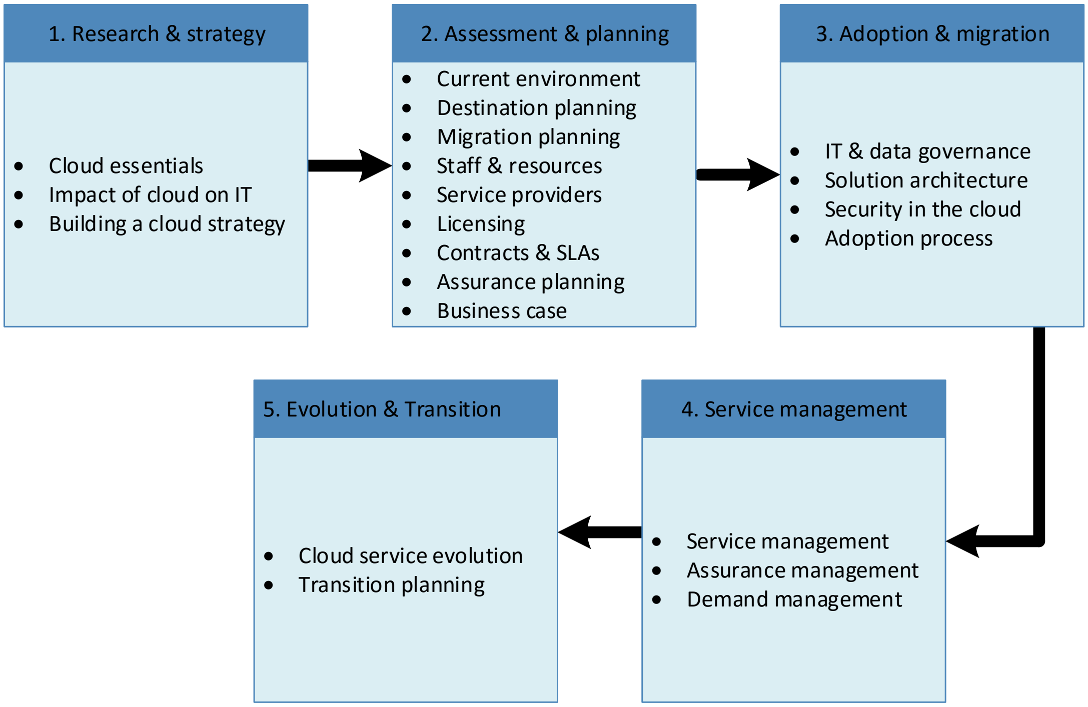
a. The first phase will involve understanding cloud services from agencies business perspective and the impact of adopting cloud on existing IT

b. The second phase for the agencies will be the assessment of the existing IT environment with an understanding of the business processes, existing application landscape and planning for the destination with an understanding of migration scenarios, required staff and resources, support from service providers and so on to create a business case for adoption

c. The adoption and migration stage will involve defining the IT and data governance architectures, and policies with solution architectures and defining and understanding the security in the cloud

d. The next phase is the service management where the agencies should work with the provider to manage the assured SLAs of the agencies. At any time the agencies might have a requirement for additional resources and as cloud is focused on availability of on-demand resources. For any compromise or failure in service delivery the provider should have set mechanisms to inform and update the agencies about the nature of failure and the impact

e. Cloud as a service has evolved over the years and the agencies should work with the provider to understand how the provider cloud has and will evolve for processes and technologies as per the requirements of the agencies and compliances. Once this is clearly documented the agencies and the providers should work towards the migration of services.



1. Research & strategy

- Cloud essentials
- Impact of cloud on IT
- Building a cloud strategy

2. Assessment & planning

- Current environment
- Destination planning
- Migration planning
- Staff & resources
- Service providers
- Licensing
- Contracts & SLAs
- Assurance planning
- Business case

3. Adoption & migration

- IT & data governance
- Solution architecture
- Security in the cloud
- Adoption process

4. Service management

- Service management
- Assurance management
- Demand management

5. Evolution & Transition

- Cloud service evolution
- Transition planning

Exhibit 14 - Roadmap for Cloud Adoption

6.6 SLAs FOR THE CLOUD

Cloud Service Level Agreements (SLAs) will help the IT and business stakeholders analyse cloud service agreements when considering different providers for adopting cloud. The SLAs will help agencies set clear expectations for service from the cloud provider and also between agencies and provider. Mentioned below are the ten important steps for SLAs in the cloud.

a. The roles and responsibilities of the agencies (consumers), providers, and any other parties involved such as carriers, etc. should be explained and stated clearly in the SLAs

b. The strategy and policies of the agencies should be considered while establishing the SLAs since there are interdependencies between the cloud services and the aspects of business

c. The levels of cloud resources and services should be understood based on the cloud service model (IaaS, PaaS, and SaaS). Each service model will have its own SLA considerations that should be clearly understood by the agencies

d. The performance objective of cloud computing usually include availability, transaction rate, response time and processing speed. The objectives should be auditable and measurable in providing levels of comfort concerning the cloud services

e. Compared to traditional IT the risks in terms of data security and privacy are considered higher and thus should be cautiously managed by the provider and the agencies. The SLAs should define a security classification scheme based on the criticality and sensitivity of data with details and data ownership, defined security levels and protection controls, and data retention and destruction policies

f. Transparent and extensible systems for monitoring the cloud services are critical to meet the expected performances. The agencies will have to validate the reporting, metering, rapid provisioning, upgrading and auditing procedures and policies with the provider

g. The agencies should request for a clear documentation of the service capabilities and performance expectations to recover/avoid a service failure. Both the provider and the agencies should prepare preventive and corrective actions in order to anticipate that the expected service deliveries do not occur

h. For the agencies, the provider should offer a BCP with a focus on the technology processes for the IT components. The level of details of the DR plan should be justified from the business objectives and the criticality of the cloud services for the agencies

i. The agencies and providers should decide upon an effective management plan which can be fulfilled via routine meetings, coordination, and escalation mechanisms to ensure that identified problems are handled properly

j. If the expectation of agencies are not achieved or due to other factors the service cannot be continued, both the agencies and provider should refer to exit SLAs which should have defined exit procedures. The exit procedures should ensure that the business continuity will not be disrupted, such as the agencies data can be preserved and transferred to other providers or to the agencies owned data centre.

6.7 COST FACTORS FOR CLOUD

Cloud delivers computing as a service our utility. The cloud will allow agencies to shed some of their expensive IT infrastructure and shift computing costs to more manageable operational expenses. The agencies will also benefit from the technological burden involved with IT systems support and maintenance. Cloud however has some upfront investment and recurring costs which the agencies should keep in mind and are mentioned as below.

a. Upfront costs which will consist of the initial investment required to setup the cloud.

   i. Technical readiness costs to accommodate the network installation or to upgrade certain components required for the connectivity to the cloud

   ii. Implementation and integration: professional services needed to manage transition to cloud and integrate it with the agencies in-house or other cloud services (hybrid cloud)

iii. **Configuration/customization:** costs to configure any agency based SaaS applications

iv. **Training:** resources required to manage the cloud providers and services

v. **Organizational change:** processes required to accommodate the cloud specific needs such as internal audit, change management, monitoring, etc.

b. Recurring costs which are related to the routine fees and support to maintain the use of cloud services.

i. **Subscription fees:** agreed on periodic fee for the subscription of cloud services (pay as you go)

ii. **Change management:** costs incurred when requesting system changes

iii. **Vendor management:** costs related to routine monitoring on cloud service provider activities, SLA, and other evaluation

iv. **Cloud coordination:** costs to manage the coordination between clouds (in case of more than one cloud provider)

v. **End user support and administration:** costs that are still retained in the agencies

vi. **Risk mitigation:** efforts required to reduce the risks to acceptable levels

vii. **Downsize/upsize:** costs related to upscale or downscale of computing resources (elasticity).

7 Links and Interdependencies

The framework for cloud adoption will have dependencies on the below policies and frameworks

a. Website and Hosting Policy for government entities in Oman.

b. Information Security policies for protection of data and information which is one of the most valuable assets for the agencies of Oman. The information security management guidelines will help protect data from any unauthorized access and modification and ensure information is available at the right time to the right people

c. OeGAF - Technical Reference Model (TRM) to provide guidance towards adoption of technical standards and best practices to manage the integration and interoperability of IT across all agencies of Oman.

8 APPENDIX A - CLOUD HOSTING/COMPUTING REQUIREMENTS

(Contractual Obligations)

Government agencies must ensure following requirements in contracts with third party Cloud Service Provider (CSP).

1. Security Requirements - The CSP offering cloud services to government agencies shall apply the appropriate set of controls to ensure compliance to security standards including but not limited to:
   - ISO/IEC 27001,
   - ISO/IEC 27017,
   - ISO/IEC 27018,
   - Cloud Security Alliance (CSA) – Control Matrix.
   - PCI-DSS Compliance - for hosting Online Payment Solutions.
2. Privacy Requirements - CSP shall be responsible for the following privacy and security safeguards:
   a. To the extent required to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the Government access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.

   b. If new or unanticipated threats or hazards are discovered by either the Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

   c. The CSP shall also comply with any additional privacy requirements required by the government.
3. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the CSPs' IT environment being used to provide or facilitate services for the Government. CSP shall be responsible for the following privacy and security safeguards:
   a. The CSP shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the CSP under this contract or otherwise provided by the Government. Exception ?

   b. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the CSP shall afford the Government access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to:

i. Authenticated and unauthenticated operating system/network vulnerability scans

ii. Authenticated and unauthenticated web application vulnerability scans

iii. Authenticated and unauthenticated database application vulnerability scans

iv. Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

If the CSP chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

4. Sensitive Information Storage And Processing - Government data and/or information must only be hosted/transacted/processed with in the geo boundaries of Sultanate of Oman. This includes the primary storage as well as the backup or disaster recovery arrangements.
   Sensitive information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The CSP shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following agreed Media Sanitization methods.
   The CSP shall develop and maintain plan for disengagement and transition of services - in case agency is transitioning to a new CSP or alternatively bringing the services back in-house.
   Agreement for retrieval/return of all data (including the primary storage as well as the backup or disaster recovery arrangements), in case of disengagement, in formats approved by the agency.

5. Protection Of Information –

   a. The CSP shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The CSP shall also protect all Government data, equipment, etc. by treating the information as sensitive. It is anticipated that this information will be gathered, created, and stored within the primary work location. If CSP personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets.

b. The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

c. The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The CSP shall ensure that the facilities that house the network infrastructure are physically secure.

d. The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The CSP shall provide requested data at no additional cost to the government.

e. No data shall be released by the CSP without the consent of the Government in writing. All requests for release must be submitted in writing to the agency representative.

6. Confidentiality And Nondisclosure –

a. The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the CSP in the performance of this contract, are the property of the Government of Oman and must be submitted to the contracting agency at the conclusion of the contract.

b. The Government of Oman has unlimited data rights to all deliverables and associated working papers and materials.

c. All documents produced for this project are the property of the Government of Oman and cannot be reproduced, or retained by the CSP. All appropriate project documentation will be given to the agency during and at the end of this contract.

d. The CSP shall not release any information without the written consent of the Contracting Officer.

e. Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

f. Additionally, any information made available to the CSP by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the CSP assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its sub-contractor shall be under the supervision of the CSP or the CSP's responsible employees. Each officer or employee of the CSP or any of its sub-contractor to whom any Government record may be made available or disclosed shall be notified in writing by the CSP that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by [mention applicable/relevant law clauses here].

9 Appendix B - Risk Assessment

When a program to develop and deploy a new business solution is being considered, there are risks associated with it, which will affect the ability of the solution to achieve its objectives.

Assessing cloud computing adoption risks involves considering a number of complex inter-related factors. Assessment of cloud adoption risks will involve conducting interviews with providers, questionnaire gathering documentation and reviews, group discussions with providers.

The challenges to cloud adoption lie in things such as location of data, exiting cloud services/provider, the number of parties involved in cloud services and surveillance from agencies.

The level of risk will vary significantly based on the type of cloud architecture being considered. Risks identified can be classified as below:

a. Compliance risks

b. Strategic risks

c. Operational risks

d. Market and finance risks.

The below exhibits are model templates and can be customized as suitable by the respective agency. The first exhibit covers the various risk domains with the likelihood and impact of associated risk. The second exhibit is a questionnaire of assessment of risks with respect to privacy, security, compliance, governance, etc.

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
Compliance Risks	Governance & Enterprise Risk Management	Lack of effective internal information security governance, risk management and compliance, and alignment with the provider own security governance	Likely	Mild
	Legal Issues : Contracts and Electronic Discovery	Storage, processing, disclosure to third-party, transfer to other legal jurisdictions of personal data and the risk for the provider not being able to produce	Expected	Severe

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
		business data in case of subpoena.		
	Incident Response	Failure for the provider to detect, handle incidents and report them to the agencies with data that can be analysed easily to satisfy legal requirements in case of forensic investigations	Likely	Serious
	Storage of data in multiple jurisdictions and lack of transparency	Mirroring data for delivery and redundant storage without actualized information as to where the data is stored. Agencies may unknowingly violate regulations especially if clear information is not provided about the jurisdiction of storage	Expected	Serious
	Compliance and Audit Management	Risk of failing to comply with government-mandated and industry-specific regulations and standards, and failure to get audit information from the provider	Likely	Serious
	Data Protection Risks	Risk of adequate Data Protection no longer being maintained to a compliant level	Likely	Serious
	Sensitive Media Sanitization	Media cannot be physically destroyed, cannot be properly identified or no adequate procedure in place	Highly Likely	Serious
	Audit or Certification unavailable	The system cannot be audited and/or certified as it should	Likely	Serious
	Compliance Degradation	Failure in achieving or maintaining Compliance (to	Likely	Serious

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
		regulation, governance, standards)		
	Governance Degradation	The agencies might cede control to the provider on a number of issues which may affect overall governance	Highly Likely	Serious
Strategic Risks	Information Management and Data Security	Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage	Likely	Serious
	Interoperability and Portability	Unable to make business applications interoperate between providers and lack of standards to minimize the risk of vendor lock-in	Likely	Serious
	Poor Provider Selection	Selection of technology or service provide sub-optimal, resulting in system operational degradation	Not Likely	Serious
	Organizational Readiness	Unable to achieve strategic alignment, cultural and workforce readiness, championship, and stakeholder buy-in	Not Likely	Serious
	Lack of Supplier Redundancy	Unable to identify / contract an alternative supplier source	Highly Likely	Serious
	Lock-In	Risk associated with the migration from an in-house IT environment to an external Provider, and from one provider to another	Likely	Serious
	Data classification on agencies side	Inappropriate data classification and definition of mitigating controls leading to being unable	Highly Likely	Serious

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
		to define requirements towards the provider		
	Data migration from on premise into the cloud (regardless whether public, private or hybrid)	Difficulty to move legacy data into a cloud based environment	Likely	Serious
Operational Risks	Data Centre Operations	Failure for the provider to respect management standards and best practices and implement security controls in accordance to sensitivity of business services	Likely	Serious
	Log & Tracing failure	Loss or Compromise of Operational Logs (including Security Logs)	Not Likely	Serious
	Backup Failure	Misplacement or theft of Backup information	Likely	Serious
	Information Management and Data Security	Loose identification of sensitive data or protection of data in transit or stored in the cloud, and prevention of data leakage	Likely	Serious
	Impact on current internal operational procedures	Review of existing operational procedures regarding change management, incident/problem management, business continuity management	Likely	Serious
	Inaccurate modelling of Resource Usage / Resource Exhaustion	Temporary failure to provide additional capacity and/or to meet Service Level Agreement.	Not Likely	Serious

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
	Integration into existing business solutions	Difficulty of Integration into legacy/current environment (interfaces)	Likely	Serious
	Malicious Activities from an Insider	Privileged users (e.g. Administrator) performing unauthorized activities on the system (data theft, tampering…)	Likely	Serious
	Sensitive Information Leakage	Accidental or Malicious activity leading to sensitive information being exposed to otherwise unauthorised group	Likely	Serious
	Operations management	Provider performs operations in a manner not meeting compliance requirements (e.g. Change management, patch management)	Likely	Serious
	Subpoena and e-discovery	Confiscation of critical system as a result of subpoena by law-enforcement agencies or civil suits	Likely	Serious
	Unauthorized access to premises	Unauthorized access to premises Including physical access to machines and other facilities	Likely	Serious
	Theft of Computer Equipment	Systems or Data be stolen	Likely	Serious
	Security of the endpoint (e.g. laptop, pc, smartphone, slate) from which the cloud service is consumed.	Inability to provide adequate policies/controls to secure the end-point	Not Likely	Serious

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
	Human Resource Constraints	Inability to find and retain the right resources to ensure service and support	Slight	Serious
	Natural Disasters	Handling of Natural Disaster Situations (Business Continuity Management)	Likely	Serious
	Licensing Risks	Unable to handle Natural Disaster Situations (Business Continuity Management)	Not Likely	Serious
	Traditional Security, Business Continuity and Disaster Recovery	Failure for the provider to implement data centres security, business continuity and disaster recovery plans	Likely	Serious
Market & Finance Risks	Loss of reputation	In-house system: risk of some significant and public incidents / In the Cloud: risk with Cloud Provider or co-tenant activities	Highly Likely	Serious
	Service Termination or Failure	The Service can no longer be provided as assumed	Likely	Serious
	Isolation Failure	Access to the Service is temporarily denied, possibly leading to reputational, critical or financial issues	Likely	Serious
	Capacity Management	Inadequate Resource Provisioning and Investment in Infrastructure	Likely	Serious
	Environment Agility / Time to Market	Latency or overall difficulty in being able to adjust the systems' characteristics (performance, architecture, segregation) to address dynamic environment	Slight	Serious
	Incident Response	The provider could not detect, handle incidents and report them to the agencies with data	Likely	Serious

RISK FRAMEWORK TEMPLATE				
Risk Domain	Risk Control Area	Description	Risk Likelihood	Risk Impact
		that can be analysed easily to satisfy legal requirements in case of forensic investigations		

Exhibit 15 - Risk Domains

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
	Value, Criticality and Sensitivity of Information
1	Who is the owner of the information?
2	What are the agencies business processes that are supported by the information?
3	What is the security classification of the information based on the agencies guidelines for protection of official information?
4	Are there any specific concerns related to the confidentiality of the information that will be stored or processed by the cloud service?
5	Does the data include any personal information?
6	Who are the users of the information?
7	What permissions do the users require to the information? (i.e. read, write, modify and/or delete)
8	What legislation applies to the information?
9	What contractual obligations apply to the information? (E.g. Compliant with a set of standards, etc.)
10	What would the impact on an agency be if the information was disclosed in an unauthorised manner?
11	What would the impact on the agency be if the integrity of the information was compromised?
12	Does the agency have incident response and management plans in place to minimise the impact of an unauthorised disclosure?
13	What would the impact on the agency be if the information were unavailable?
13.a	What is the maximum amount of data loss that can be tolerated after a disruption has occurred?
13.b	What is the maximum period of time before which the minimum levels of services must be restored after a disruption has occurred?
13.c	What is the maximum period of time before which the full service must be restored to avoid permanently compromising the business objectives?
	Data Sovereignty
14	Where is the registered head office of the cloud provider?
15	Which countries are the cloud services delivered from?
16	In which legal jurisdictions will the agency's data be stored and processed?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
17	Will the cloud provider allow the agencies to specify the locations where their data can and cannot be stored and processed?
18	Does the service have any dependency on any third parties (e.g. outsourcers, subcontractors or another cloud provider) that introduce additional jurisdictional risks? If yes, can the cloud provider provide the following details for each third party involved in the delivery of the service?
18.a	The registered head office of the third party.
18.b	The country or countries that their services are delivered from.
18.c	The access that will have to agency data stored, processed and transmitted by the cloud service
19	Have the laws of the country or countries where the data will be stored and processed been reviewed to assess how they could affect the security and/or privacy of the information?
20	Do the laws actually apply to the cloud provider and/or its customer's information? (E.g. some privacy laws exempt certain types of businesses or do not apply to the personal information of foreigners.)
21	Do the applicable privacy laws provide an equivalent, or stronger, level of protection?
21.a	If no, will the agencies be able to negotiate with the cloud provider to ensure that the equivalent privacy protections are specified in the contract?
22	How does the cloud provider deal with requests from regulatory agencies to access agency information?
22.a	Will the provider only disclose information in response to a valid court order?
22.b	Will the provider inform the agency if they have to disclose information in response to such a request?
22.c	Is the provider prevented from informing customers including agencies that they have received a court order requesting access to their information?
	Privacy
23	Can the agencies do a Privacy Impact Assessment (PIA) for the provider to identify the privacy risks associated with the use of the cloud service together with the controls required to effectively manage them? Or will the provider comply with the privacy requirements of the agencies?
24	Is the cloud provider's use of personal information clearly set out in its privacy policy?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
24.a	Is the cloud provider's privacy policy consistent with the agency’s business requirements?
25	Will the cloud provider notify the agencies if their data is accessed by, or disclosed to, an unauthorised party?
26	Who can the agency, its staff and/or customers complain to if there is a privacy breach?
	Governance
	Terms of Service
27	Will the cloud provider negotiate contracts with the agencies or must they accept a standard Terms of Service?
28	Will the cloud provider’s Terms of Service and SLA clearly define how the service protects the confidentiality, integrity and availability of all agency information entrusted to them; especially official information; and the privacy of all personally identifiable information?
29	Will the cloud provider’s Terms of Service specify that the agency will retain ownership of its data?
30	Will the cloud provider use the data for any purpose other than the delivery of the service?
31	Is the cloud provider’s service dependent on any third-party services?
	Compliance
32	Will the cloud provider’s Terms of Service allow an agency to directly audit the implementation and management of the security measures that are in place to protect the service and the data held within it?
32.a	If yes, does this include performing vulnerability scans and penetration testing of the service and the supporting infrastructure?
32.b	If no, does the cloud provider undergo formal regular assessment against an internationally recognised information security standard or framework by an independent third-party? (E.g. are they certified as being compliant with ISO/IEC 27001? Have they undergone an ISAE 3402 SOC 2 Type II assessment?)
33	Will the cloud provider allow an agency to thoroughly review recent audit reports before signing up for service? (E.g. will the cloud provider provide the Statement of Applicability together with a copy of the full audit reports from their external auditor, and the results of any recent internal audits?)

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
34	Will the cloud provider enable potential customers to perform reference checks by providing the contact details of two or more of its current customers?
35	Has the cloud provider published a completed Cloud Computing Code of Practice?
	Confidentiality
	Authentication and Access Control
36	Will the cloud service support the agency's identity management strategy?
37	Does the cloud provider have an effective internal process that ensures that identities are managed and protected throughout their lifecycle?
38	Does the provider have an effective audit process that is actioned at regular intervals to ensure that user accounts are appropriately managed and protected?
39	Are the controls required to manage the risks associated with the ubiquitous access provided by the cloud been identified?
39.a	Does the cloud service meet those control requirements?
40	Are all passwords encrypted, especially system/service administrators, in accordance with complexity requirements?
	Multi-Tenancy
41	Will the cloud provider allow the agency to review a recent third-party audit report (e.g. ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of the security controls and practices related to virtualisation and separation of customer's data?
42	Will the cloud provider permit agencies to undertake security testing (including penetration tests) to assess the efficacy of the access controls used to enforce separation of customer's data?
	Standard Operating Environments
43	Are there appropriate build and hardening standards defined and documented for the service components an agency is responsible for managing?
44	Can an agency deploy operating systems and applications in accordance with internal build or hardening standards?
44.a	If no, does the cloud provider have appropriate build and hardening standards that meet any agency's security requirements?
44.b	Does the virtual image include a host-based firewall configured to only allow the ingress and egress (inbound and outbound) traffic necessary to support the service?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
44.c	Does the cloud provider allow host-based intrusion detection and prevention service (IDS/IDP) agents to be installed within the virtual machines?
45	Does the cloud provider perform regular tests of its security processes and controls?
45.a	Will they provide agencies with a copy of the associated reports?
46	Can a penetration test of the service be performed to ensure that it has been securely deployed?
	Patch and Vulnerability Management
47	Is the cloud provider responsible for patching all components that make up the cloud service?
47.a	If the cloud provider is NOT responsible for patching all components that make up the cloud service, then will it share the details for patching with responsibility?
48	Does the cloud provider's Terms of Service or SLA include service levels for patch and vulnerability management that includes a defined the maximum exposure window?
49	Will the cloud provider allow an agency to perform regular vulnerability assessments?
50	Will the Terms of Service or SLA include a compensation clause for breaches caused by vulnerabilities in the service?
50.a	If the Terms of Service or SLA includes compensation clause for breaches caused by vulnerabilities in the service, does it provide an adequate level of compensation should a breach occur?
	Encryption
51	Does the cloud service use only approved encryption protocols and algorithms?
52	Who will be responsible for managing the cryptographic keys?
53	Does the provider have a key management plan that meets the requirements of the agencies?
	Cloud provider Insider Threat
54	Will the cloud provider undertake appropriate pre-employment vetting for all staff that have access to agency data?
54.a	Does the cloud provider perform on-going checks during the period of employment?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
55	If the cloud provider is dependent on a third-party to deliver any part of their service, will the third-party undertake appropriate pre-employment vetting for all staff that have access to customer data?
56	Will the cloud provider have a SIEM service that logs and monitors all logical access to customer data?
57	Does the cloud provider enforce separation of duties to ensure that audit logs are protected against unauthorised modification and deletion?
58	Do the Terms of Service or SLA require the cloud provider to report unauthorised access to customer data by its employees?
58.a	If yes, is the cloud provider required to provide details about the incident to affected agencies to enable them to assess and manage the associated impact?
	Data Persistence
59	Does the cloud provider have an auditable process for the secure sanitisation of storage media before it is made available to another customer?
60	Does the cloud provider have an auditable process for secure disposal or destruction of ICT equipment and storage media (e.g. hard disk drives, backup tapes etc.) that contain customer data?
	Physical Security
61	If it is practical to do so, can the cloud provider's physical security controls be directly reviewed or assessed by the agency?
61.1	If no, will the cloud provider allow the agency to review of a recent third party audit report (e.g. ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of their physical security controls?
62	Do the cloud provider's physical security controls meet the minimum requirements as defined in the agencies security guidelines to protect the information stored in the cloud service?
	Data Integrity
63	Will the cloud provider provide data backup or archiving services as part of their standard service offering to protect against data loss or corruption? If not, do they offer data backup or archiving services as an additional service offering to protect against data loss and corruption?
64	How are data backup and archiving services provided?
65	Does the SLA specify the data backup schedule?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
66	Does the data back-up or archiving service ensure that business requirements related to protection against data loss are met? (I.e. does the service support the business Recovery Point Objective?)
67	What level of granularity does the cloud provider offer for data restoration?
68	What is the cloud provider's process for initiating a restore?
69	Does the cloud provider regularly perform test restores to ensure that data can be recovered from backup media?
70	Does the agency need to implement a data backup strategy to ensure that it can recover from an incident that leads to data loss or corruption?
71	Does the proposed data backup and archiving strategy support the agency in meeting its obligations?
	Availability
	Service Level Agreement
72	Does the SLA include an expected and minimum availability performance percentage over a clearly defined period?
72.a	If the SLA include an expected and minimum availability performance percentage over a clearly defined period, are the agencies business requirements for availability met? I.e. does the service support the business's Recovery Time Objective and Acceptable Interruption Window?
73	Does the SLA include defined, scheduled outage windows?
73.a	If the SLA includes defined, scheduled outage windows, do the specified outage windows affect business operations?
73.b	If the SLA does NOT include defined, scheduled outage windows, has the cloud provider implemented technologies that enable them to perform maintenance activities without the need for an outage?
74	Does the SLA include a compensation clause for a breach of the guaranteed availability percentages?
74.a	If the SLA include a compensation clause for a breach of the guaranteed availability percentages, does this provide an adequate level of compensation should the cloud provider breach the SLA?
	Denial of Service Attacks
75	Does the cloud provider utilise protocols and technologies that can protect against DDoS attacks?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
75.a	If yes, does enabling the cloud provider's DDoS protection services affect the answer to questions 15, 16 and 17?
76	Can the agency specify or configure resource usage limits to protect against EDoS/bill shock?
	Network Availability and Performance
77	Do the network services directly managed, or subscribed to by the agency provide an adequate level of availability?
78	Do the network services directly managed, or subscribed to by the agency provide an adequate level of redundancy/fault tolerance?
79	Do the network services directly managed, or subscribed to by the agency provide an adequate level of bandwidth (network throughput)?
80	Is the latency between the agency network(s) and the cloud provider's service at levels acceptable to achieve the desired user experience?
80.a	If no, is the latency occurring on the network services directly managed, or subscribed to by the agency?
80.b	Can the issue be resolved either by the network cloud provider or the agency?
81	Is the packet loss between the agency network(s) and the cloud provider's service at levels acceptable to achieve the desired user experience?
81.a	If no, is the packet loss occurring on a network services directly managed, or subscribed to by the agency?
81.b	Can the issue be resolved either by the network cloud provider or the agency?
	Business Continuity and Disaster Recovery
82	Does the cloud provider have business continuity and disaster recovery plans?
83	Will the cloud provider permit the agency to review of its business continuity and disaster recovery plans?
84	Do the cloud provider's plans cover the recovery of the agency data or only the restoration of the service?
85	If the cloud provider's plans cover the restoration of agency data, is the recovery of customer data prioritised?
85.a	If so, how? Will agencies be prioritised based on size and contract value?
86	Does the cloud provider formally test its business continuity and disaster recovery plans on a regular basis?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
86.a	If yes, how regularly are such tests performed?
86.b	Will the provider provide agencies with a copy of the associated reports?
	Incident Response and Management
87	Does the cloud provider have a formal incident response and management process and plans that clearly define how they detect and respond to information security incidents?
87.a	If yes, will they provide the agency with a copy of their process and plans to enable it to determine if they are sufficient?
88	Does the cloud provider test and refine its incident response and management process and plans on a regular basis?
89	Will the cloud provider engage the agencies when testing its incident response and management processes and plans?
90	Does the cloud provider provide its staff with appropriate training on incident response and management processes and plans to ensure that they respond to incidents in an effective and efficient manner?
91	Does the cloud provider's Terms of Service or SLA clearly define the support they will provide to the agency should an information security incident arise?
91.a	Will the cloud provider notify agencies when an incident that may affect the security of their information or interconnected systems is detected or reported?
91.b	Specify a point of contact and channel for agencies to report suspected information security incidents?
91.c	Define the roles and responsibilities of each party during an information security incident?
91.d	Provide agencies with access to evidence (e.g. time stamped audit logs and/or forensic snapshots of virtual machines etc.) to enable them to perform their own investigation of the incident?
91.e	Provide sufficient information to enable the agency to cooperate effectively with an investigation by a regulatory body?
91.f	Define which party is responsible for the recovery of data and services after an information security incident has occurred?
91.g	Share post incident reports with affected agencies to enable them to understand the cause of the incident and make an informed decision about whether to continue using the cloud service?

RISK ASSESSMENT QUESTIONNAIRE	
Q No	Question
91.h	Specify in the contract limits and provisions for insurance, liability and indemnity for information security incidents?
92	Does the cloud providers incident response and management procedures map to (or fit with) the agency internal policy and procedures; that does not hinder or delay the agency's ability to manage incidents in a timely and effective manner?

Exhibit 16 - Risk Assessment Questionnaire