U.S. DEPARTMENT OF
ENERGY
Office of the Chief
Information Officer

DOE Cloud Smart Reference Guide

June 13, 2019
Version 2

Office of the Deputy CIO for Architecture, Engineering, Technology
& Innovation, IM-50

Revision History

Version	Date	Author
1.0	February 7, 2019	Office of Architecture, Engineering, Technology & Innovation (IM-50)
1.12	May 6, 2019	Office of Architecture, Engineering, Technology & Innovation (IM-50)
2.0	June 13, 2019	Office of Architecture, Engineering, Technology & Innovation (IM-50)

Table of Contents

1 Executive Summary

This *DOE Cloud Smart Reference Guide* is a resource that should be referenced when formulating actionable, practical cloud adoption and implementation strategies. It is a collection of proven guiding principles offering insights for strategic facilitation of transformation planning, architecture definition, business process integration, and organizational change. This reference guide is rooted in both government and commercial best practices and centers around applied experiences. The intent is not to replay the Cloud Smart policy [1], but rather afford you a sample of referential experiences, lessons learned and best practices that can be readily applied.

Cloud adoption is a powerful IT and mission enabler: the prospect of additional on-demand compute resources for a period of high demand, where performance and productivity would otherwise suffer, is an example of a very impactful feature. An application can be deployed utilizing cloud-based DevOps pipelines, compute can be automatically scaled to meet consumption needs, and then monitored with native cloud tools. Automated demand-based detection also provides for instantaneous release of those elastic resources when the peak has subsided.

These are just a few of the value propositions that you can realize through practical application of the methodologies and strategic guiding principles laid out in this *DOE Cloud Smart Reference Guide*. It is important to note that a jump into cloud without adequate transformational strategy often results in higher initial cloud costs and the inability to realize the full return on your investment (ROI), such as easier integration of your targeted SaaS solutions, deployment as PaaS, and legacy IT modernization.

Depending on where you are in your journey, cloud transformations can be a complex undertaking. It must be approached with deliberative planning and execution. Transformation involves shifts in IT and mission value assessment, analysis, technologies, architecture, development, operations, personnel skills, and end-to-end enterprise processes. Smart cloud adoption embellishes moving workloads to another environment, it involves application and legacy process changes.

Each organization within the Department works with many vendors, each with its own requirements and specifications. With that in mind, the DOE Cloud Smart Reference Guide will not reference a particular vendor as a solution, but rather provide a selection methodology to aide in the selection in a Cloud Service Provider (CSP). It is important to consider vendor affinities when selecting a CSP. For example, an organization may have considerable amount of applications with Vendor 1. It is important to consider Vendor 1 as a CSP as well, which may allow for cost avoidance. If a different vendor is chosen over Vendor 1, it is possible that hidden costs may arise. This guide will provide the logical methodology in selecting the CSP regardless of vendor preference or affinity.

The Department of Energy recognizes enterprise architecture (EA) as an evolutionary asset and practice, which IT organizations must orient towards delivery of innovative, business-focused services and capabilities. Without this strategic evolution, the process of designing, building, and operating advanced, integrated, and effective systems is exceedingly difficult.

[1] https://cloud.cio.gov/

2 Purpose

The purpose of this guide is to advise organizations in the Department through development or vetting of a cloud strategy and implementation plan. The content is multi-faceted: overarching guidance for strategizing and applying solution adoption as enabled by select Cloud Service Providers (CSPs); encompasses Cloud Smart policies; provides considerations for addressing key Federal IT Acquisition Reform Act (FITARA) and Data Center Optimization Initiative (DCOI) requirements; and it contains Department of Energy best practices for data driven architecture and innovation equipping organizations to meet IT modernization and timely data center exit goals.

The intended user of the DOE Cloud Smart Reference Guide is for any organization in the Department interested in evaluating cloud adoption strategies. Some organizations may uses this Guide as part of their on-premises data center foot print reduction and consolidation efforts, others may use it in in search of smart strategies and lessons learned from others as they embarked upon the journey. In keeping with OCIO guidance, this Guide steps through discovery of opportunities and development of rationale for workloads meeting certain criteria to be migrated using a hybrid cloud approach, co-located to more advanced data centers, or remain in an on-premises cloud. Yes, there are a few workloads that should probably remain on-site.

This Guide provides explanation and recommendations regarding how to:

- Evaluate requirements and organizational needs for selection of private, hybrid and public cloud.
- Consider applicable cloud types (i.e. IaaS, PaaS, SaaS).
- Evaluate public and hybrid cloud services provided by select Cloud Service Providers (CSPs)
- Enable migration of workloads to existing cloud platforms
- Define Key Cloud Adoption and Migration Considerations

3 Scope

While adaptable to organizations considering cloud adoption or exploring opportunities to further implementations, this Guide includes a use case with a named vendor as an example of how a DOE organization has migrated to the cloud. This use case can be found in Appendix 3. The principles can be applied at any point in the cloud adoption and implementation journey. Whether just starting out or if there are workloads already in cloud, guidance is provided in each of the key aspects presented.

4 Introduction

Cloud brings extraordinary features such as always-on-availability, capacity elasticity, pay-as-you-go, automation for performance assurance, transparent refresh management, economically practical Disaster Recovery (DR) and Continuity of Operations (COOP), to name a few. However, as this Guide illuminates, without adequate consideration of the implications of proper strategies for modernization and transformation, development, operations planning and processes, a jump into cloud can be highly impactful with potentially unintended consequences. Key factors to consider include:

- Costs and value realization
- Recognition of organizational, processes, policies, and workforce skills transformational implications
- Recognition of cloud efficiencies
- Security and operational visibility
- Data sensitivity, privacy and co-mingling of data
- Potential consequence of having to consider exiting cloud due to adoption issues
- Records management, including capture, maintenance, access, protection and disposition

Potential cost avoidance (legacy on-premises or co-location hosting situations requiring routine capital expenditure outlays, infrastructure refreshes, overbuild requirements to meet short-lived instantaneous demands, to name a few) is a primary motivator for cloud adoption. The usual assumption is that migration of on-premises hosting to cloud will result in cost savings. In reality, a jump into cloud without adequate transformational strategy often results in higher initial cloud costs and the inability to realize some inherent added values of cloud.

While Cloud Service Providers calculators accept difficult to estimate variables such as egress data volumes, there is usually no basis for actuals in the legacy state on-premises architectures. Only a study of the target state cloud architecture and interconnectivity and communications of on-premises and cloud interdependent applications can lead to estimates of cloud egress data volume. Due to the nature of how CSP's structure their cost models, egress data volume can be a significant 'hidden' monthly cloud cost. Strategies to fully explore refactoring opportunities and to accurately estimate cloud Total Cost of Ownership (TCO) are highly recommended.

Recognizing the transformational impact of the cloud services model on the organization, a multi-phased cloud adoption strategy that goes beyond technology implementation and addresses all of the major operational areas of the IT organization should be considered, including:

- Cloud-optimized Re-Architecture
- Policies and processes transformation, as well as automation, that support cloud
- Development and implementation of a governance model
- Workforce skillsets realignment
- Active collaboration with Cyber Security

In the various explanations in this Guide, on-premises is often referred to as the facility in which infrastructure is 'housed' – in an organization's data center or a co-location facility. For clarity, 'legacy' (non-cloud infrastructure) is used to describe traditional on-premises data center facilities consisting of physical hardware, virtualization platforms, appliances, network, air, power, etc. As will be seen, private cloud and hybrid cloud components can be housed in an organization's data center or co-location.

In this Guide you will find references to DevSecOps. That is because cloud is an enabler of a continuous integration and delivery (CI/CD) platform. Rather than the traditional model where Commercial Off the Shelf (COTS) applications are configured or customized, or applications go through a development life-cycle, and then are passed off to Security for Authority To Operate (ATO) approval, there's best-practice opportunity to transform to "DevSecOps" leveraging agile sprints to drive a high degree of collaboration between Development, Cyber Security and Operations. This results in faster time to value, 'secure by design', and faster problem resolution.

Unlike the traditional on-premises and co-location computing models, cloud offers on-demand, scalable, elastic, and reserved consumption options, with associated operational and cost efficiencies. These can consist of any desired mix of resources and services available to workload execution, whether it be compute capacity, network bandwidth, utilization hours, etc. When appropriately architected, designed and implemented, cloud services and resources can be highly customized and configured to yield extraordinary resources flexibility and cost efficiencies. These factors can be amplified through strategies such as automation, cloud optimization, reusable micro services, among others.

For example, in the best of on-premises compute situations, virtual host infrastructure is essentially "assigned" workloads for which it must be available, usually 24 X 7, and at capacities that peak demands dictate. Further, the vast majority of Federal Missions do not subject workloads to "follow-the-sun utilization". Hence, much of the provisioned capacity will run idle during US non-working hours of the day. By incorporating scalable cloud services into the design that automatically reduce compute capacity to the least amount necessary to support the workload at any given time, or de-provision non-production capacity during non-working hours, significant savings can be realized.

Change agents tasked with initiating and implementing the fundamental shifts in how IT and Mission organizations function are generically referred to throughout this guide as 'practitioners'. Examples of practitioner functions are:

- Envisioning: thinking "big-picture" (Mission/Business and Operations leaders, Enterprise Cloud Architects, etc. who lead transformation.
- Influencing: Driving Enterprise Architecture policies and standards.
- Evangelizing: Creates, promotes, and institutionalizes cloud best practices across the organization.
- Enabling: Develops cloud migration factory capabilities.
- Leading: Set the example with workforce skills re-development planning and execution.
- Guiding: As cloud experts, enable maximized recognition of cloud efficiencies and mitigation of cloud exit risk due to adoption failure.

Only through strategic discovery and analysis of the factors and incorporating them into adoption decision making is it possible to achieve Cloud Smart adoption. There is other guidance ahead in this *DOE Cloud Smart Reference Guide* to help maximize your adoption strategy.

4.1 Relevant Federal Policies & Guidelines

Federal policies and guidelines should be considered when establishing a cloud strategy. This Guide suggests practical ways to accomplish this including applied case studies.

4.1.1 FITARA and DCOI

The Federal Information Technology Acquisition Reform Act (FITARA) and the Data Center Optimization Initiative (DCOI) are federal mandates to consider when planning cloud adoption.

4.1.1.1 FITARA

FITARA is a major overhaul of Federal Information Technology policy passed by Congress in December 2014. It is a law that aims to change and reform the current framework that manages how the federal government buys new technology.

It requires agencies to report the following to OMB:

- Comprehensive inventory of data centers
- Strategy to consolidate and optimize data centers, including performance metrics, timelines, investment and cost savings plans
- Quarterly progress reports on the agency's strategy

4.1.1.2 DCOI

The Data Center Optimization Initiative (DCOI) requires agencies to:

- Develop and report their data center strategies
- Transition to more efficient infrastructure, such as cloud services and inter-agency shared services
- Leverage technology advancements to optimize infrastructure, and
- Provide quality services for the public good

In complying with DCOI, sustainability, optimization and utilization objectives can be met. If private cloud meets these objectives, they are not in and of themselves drivers for migration to public or hybrid cloud.

4.1.2 Cloud Smart Policy

In 2010, the Federal Government created the Cloud First strategy. As technology advanced and cloud adoption uptake increased, Cloud First evolved to the new policy called Cloud Smart. Agencies are encouraged to perform and leverage a full system and application rationalization, including whether virtualization, containerization, and other modern practices can be leveraged to increase efficiency in agency-owned data centers and vendor offerings.

In alliance with FITARA, DCOI and the Cloud Smart policy, this reference guide encourages a more risk-based approach to cloud adoption and integration, securing systems that place appropriate emphasis on continuous data-level protections and awareness, and that fully leverage modern virtualized technologies. Additionally, it is critical that agencies have comprehensive visibility of their data, both on-premises and in the cloud, and perform continuous monitoring in order to detect malicious activity.

Other considerations are: security, procurement and workforce. Examples of how each of these can be applied are given throughout this Guide. How the considerations are applied are dependent upon circumstances and strategy.

4.1.3 Federal Records Laws and Regulations

The management of Federal records is informed by several key references that include among them:

4.1.3.1 Presidential & Federal Records Act Amendments of 2014 (P.L. 113-187)

The Act provides additional requirement for records beyond the Federal Records Act of 1950, and includes a revised definition of a Federal record to cover "recorded information, regardless of form or characteristics" where *recorded information* is further defined as "information created, manipulated, communicated, or stored in digital or electronic form." This definition applies to qualifying agency information held in a cloud service and the agencies using such cloud services must ensure the information therein are managed in accordance with the applicable laws and regulations governing Federal records.

4.1.3.2 "Electronic Records Management" (36 CFR Part 1222.32)

The regulations provides that agencies responsible for administering contracts must safeguard the records crested, processed or in the possession of a contractor or non-Federal entity. Consequently, the agency is responsible for the records and effective management of the same regardless of the cloud type – government or commercial.

4.1.3.3 "Managing Information as a Strategic Resources" (OMB Circular A-130)

The circular requires agencies fully incorporate records management functions, and retention and disposition requirements into information lifecycle processes and stages, particularly cloud-based services – software, platform and infrastructure.

4.1.3.4 "Managing Government Records Directive" (OMB/NARA Memorandum M-12-18)

The memorandum promotes openness and accountability, and also reduced long-term costs to agencies in keeping with many of the benefits of cloud usage. Among the more important and pressing goals it states therein is the management of all permanent electronic records in electronic format by December 31, 2019, to the fullest extent possible. This goal aligns with the NARA strategic plan for 2018-2022 that will significantly reduce the acceptance of agencies' analog records in favor of electronic formats accepted into the Federal Records Centers after December 31, 2022. Effective management of records in the cloud will help DOE prepare and respond to meet the 2019 and 2022 compliance deadlines.

4.1.3.5 "Guidance on Managing Records in Cloud Computing Environments" (NARA Bulletin 2010-5)

The bulletin provides guidance for managing records considerations in cloud computing environments. It specifically calls out that agencies remain responsible for the management of it records even in contracted environments, and the guidance offers a sample records management clause for agency use in contracts or similar agreements to, at a minimum, ensure that a Federal agency and the contractor are aware of their statutory records management responsibilities. As such, the clause cited should be coordinated with, at a minimum, the DOE Records Management Program, the Office of Management, and the Office of General Counsel to ensure appropriate consideration and inclusion in any cloud contracts or agreements.

5 Cloud Benefits and Implications

Much is written and discussed about the benefits and implications of cloud adoption and implementation. Many selections, benefits and implications of cloud and the methods to analyze them are common across CSP’s. The following describes key benefits and implications. They are expanded upon throughout the Guide.

5.1 Key Cloud Benefits

The following are key benefits that may be realized through cloud adoption and implementation

- Legacy IT modernization or retirement/sun-setting
- Faster time-to-market of solutions
- Environments ready when you need them (on demand)
- Enables optimal Return on Investments (ROI)
- Managed services including logging, monitoring, analytics, Identity & Access Management, can reduce operational costs.
- Reduced Operations and Maintenance costs
- Scalability -- Capacity elasticity and auto-scaling
- Automation for things such as performance assurance and continuous development
- Facilitates adherence to relevant federal policy and guidelines
- High availability and fault tolerance
- More economically viable Continuity of Operations (COOP) and Disaster Recovery
- Costing models supporting “pay as you go” (based on consumption)
- Periodic capitol investments in aging hardware refreshes are no longer concerns
- The most modern infrastructure and services are always available to your environment

5.2 Primary Cloud Implications

The following are the primary implications of cloud and its implementation to consider in planning.

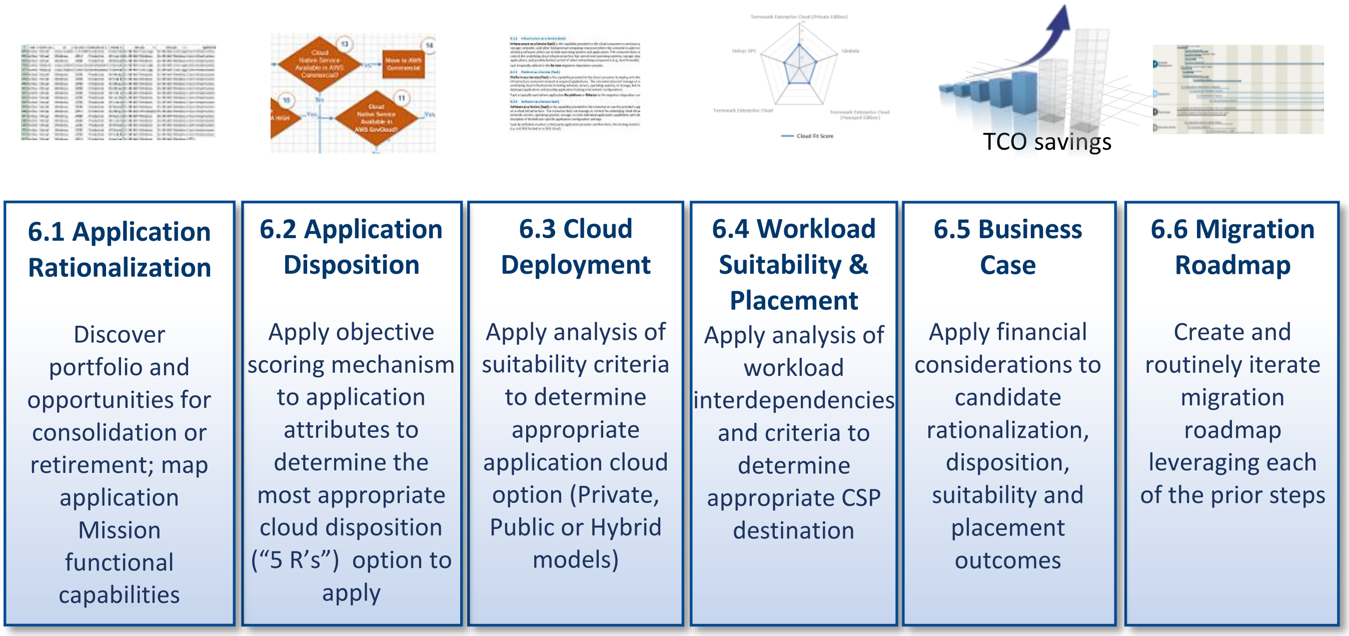
- Transformation is a complex undertaking
- Identity & Access Management and assurance levels for identity, federation, and authenticator
- Cyber Security integration
- Foreign National restriction
- US hosted necessity
- Core IT infrastructure readiness
- Requires planning and execution strategies that are quite different from traditional on-premises approaches
- Governance
- Adaptation of the financial model from periodic capital expense of shared resources to continuous consumption of individual services.

6 Enterprise Migration Strategy & Implementation Modeling

The model depicted in Figure 6-1 consists of best practice components for establishing cloud migration strategy and achieving practical implementation. A synopsis of each of the following components is provided in numbered portions of this section. Details are in sections as shown in *Table 6.1 – Enterprise Migration Strategy & Implementation Modeling Directory*. Not all require/have detailed sections – designated N/A.

Model Component	Synopsis Section	Detailed Section
Application Rationalization	6.1	N/A
Application Disposition	6.2	7
Cloud Deployment	6.3	8
Workload Suitability & Placement	6.4	9
Business Case	6.5	10
Migration Roadmap	6.6	N/A

Table 6.1 -- Enterprise Migration Strategy & Implementation Modeling Directory



6.1 Application Rationalization

Discover portfolio and opportunities for consolidation or retirement; map application Mission functional capabilities

6.2 Application Disposition

Apply objective scoring mechanism to application attributes to determine the most appropriate cloud disposition ("5 R's") option to apply

6.3 Cloud Deployment

Apply analysis of suitability criteria to determine appropriate application cloud option (Private, Public or Hybrid models)

6.4 Workload Suitability & Placement

Apply analysis of workload interdependencies and criteria to determine appropriate CSP destination

6.5 Business Case

Apply financial considerations to candidate rationalization, disposition, suitability and placement outcomes

6.6 Migration Roadmap

Create and routinely iterate migration roadmap leveraging each of the prior steps

Figure 6–1 Enterprise Migration Strategy & Implementation Model

The following explanations correspond with numbered components in Figure 6-1.

6.1 Application Rationalization

This is the process of discovering the application and workload and creating the inventory of the portfolio.

An analysis is conducted to identify opportunities for application or workload consolidation or retirement by mapping Mission functional capabilities. The methodology assesses functional redundancies (more than one application delivering the same functionality) and gaps (not meeting the Mission requirements).

6.2 Application Disposition

This is the process of objectively reviewing how well applications meet Mission and Technical values. The disposition methodology applied can be an objective attribute scoring process that enables consistent, repeatable measures and criteria to arrive at migration disposition application ranking, or can intentionally be more subjective and less formal, based on your practitioner's experience.

Whichever method is employed by the Site, Headquarters, etc., it's important to consider the numerous drivers of each method.

Migration Disposition is a driver for the *Cloud Service Model selection in Section 7.3*. The recommended application disposition methodology is covered in detail in *Section 7 – Application Disposition Methodology*. It provides guidelines and recommendations for determination of the appropriate techniques for readying workloads for the cloud. Practitioners should be consulted to factor Site requirements into the methodology.

6.3 Cloud Deployment Model

The cloud deployment model utilizes application and workload attributes based on criteria to determine appropriateness of Private, Hybrid or Public cloud options. *Cloud Deployment Model Selection and Cloud Service Model Selection (Sections 8.1 and 8.2 respectively)* are subcomponents of the Cloud Deployment Model.

They are covered in detail in *Section 8 – Cloud Deployment Model*.

6.4 Workload Suitability & Placement

The potential of an application or workload perhaps not being suitable for cloud and needing to remain in an on-premises situation or possibly being a candidate for co-location placement is considered in this section.

Placement is analysis of applications and workloads to determine either their independence or the need to apply criteria that will logically group them for transformation and migration wave planning. This is referred to as *affinity grouping*.

Workload Suitability & Placement are covered in detail in *Section 9 – Workload Suitability & Placement.*

6.5 Business Case

The business case for cloud adoption consists of all the conventional elements of a business case, which is left outside the scope of this document. There are, however, specific elements applicable to cloud that are covered here with the recommendation that they not be overlooked.

Cost models and other relevant financial considerations must be applied to candidate rationalization, disposition, deployment, suitability, and placement analysis outcomes.

Each of these, along with topics of Total Cost of Ownership (TCO), Cloud Cost Factors, and CSP Cost Calculators: What to Look Out For are covered in detail in *Section 10 – Business Case* and *Appendix 2 – OneID Cost Factors Case Study*.

6.6 Migration Roadmap

It is recommended to create a program roadmap at the outset of the initial cloud journey to include a pilot cloud adoption project consisting of aspects of each of the six components of the *Enterprise Migration Strategy & Implementation Model (Figure 2-1)*. Also in the pilot scope, include a set of workloads selected by applying criteria representing perhaps two workloads from each of the Re-host, Re-platform and Refactor categories (in case, during the process of discovery, one needs to change categories).

As success is achieved, routinely refresh your roadmap based on lessons learned, the outcomes of iterating through the above steps in the delivery model, and on the basis of increased maturity and resources re-skilling and availability. Pay particular attention to DCOI exit (on-premises data center) strategy objectives, goal dates, complexity, interdependencies, and budget.

7 Application Disposition Methodology

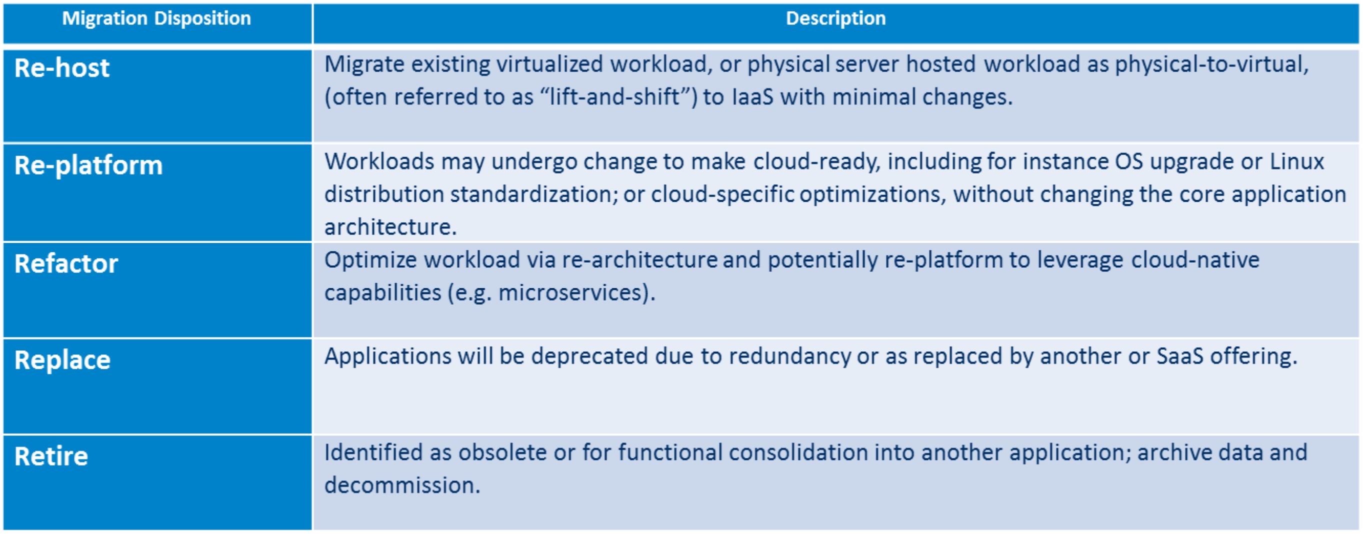
In this process of objectively reviewing how well applications meet Mission and Technical values, the disposition methodology applied can be an objective attribute scoring process that enables consistent, repeatable measures and criteria to arrive at migration disposition application ranking, or can intentionally be more subjective and less formal, based on your practitioner's experience.

Whichever method is employed by the Site, Headquarters, etc., it's important to consider the numerous drivers of each method. For instance, it may be important to a Site or Headquarters to group applications by employing a strategy of qualitative and/or quantitative objective measures that will result in the prioritization of applications and in what sequence to migrate them. Examples of prioritization might be applications with infrastructure that is due for refresh or according to funding availability for desired refactoring or replacement, etc.

Migration Disposition is a driver for the Cloud Service Model selection. The following is the detailed application disposition methodology to follow. It provides guidelines and recommendations for determination of the appropriate techniques for readying workloads for the cloud. Your practitioners should be consulted to factor site requirements into the methodology.

7.1 Application Cloud Disposition

Table 7-1 summarizes industry best practice Migration Disposition definitions. Each application that is deemed cloud suitable is classified into one of 5 cloud disposition types (known as the "5 R's"): Re-host, Re-platform, Refactor, Replace, or Retire.



Migration Disposition	Description
Re-host	Migrate existing virtualized workload, or physical server hosted workload as physical-to-virtual, (often referred to as "lift-and-shift") to IaaS with minimal changes.
Re-platform	Workloads may undergo change to make cloud-ready, including for instance OS upgrade or Linux distribution standardization; or cloud-specific optimizations, without changing the core application architecture.
Refactor	Optimize workload via re-architecture and potentially re-platform to leverage cloud-native capabilities (e.g. microservices).
Replace	Applications will be deprecated due to redundancy or as replaced by another or SaaS offering.
Retire	Identified as obsolete or for functional consolidation into another application; archive data and decommission.

Table 7-1 -- Application Disposition 5 R's

7.2 Disposition Assessment Analysis

This section defines the assessment in which applications and workloads are evaluated for appropriate disposition. That is, whether Re-host, Re-platform, Refactor, or Replacement should be undertaken. Note that a decision to Retire an application is a disposition arrived at directly, without the need for this analysis.

The decision logic as shown in the flow diagrams apply some example criteria. The criteria based on the adoption strategy should be decided upon and the decision logic and adapted accordingly. Vendor affinities are a factor in selecting a CSP. For example, if an organization has considerable Vendor 1 applications it may prove beneficial to also use Vendor 1 as the preferred CSP. The logic here is to maintain vendor affinity to save money in the long run.

Federal Information Security Management Act (FISMA) moderate or high classifications will drive vendor Government solution selection. Also, if considering another vendor, adapt the decision logic accordingly.

The analysis is conducted in two phases: *Phase 1 - Decision Matrix Analysis* leading to *Phase 2 - Disposition Option Analysis*.

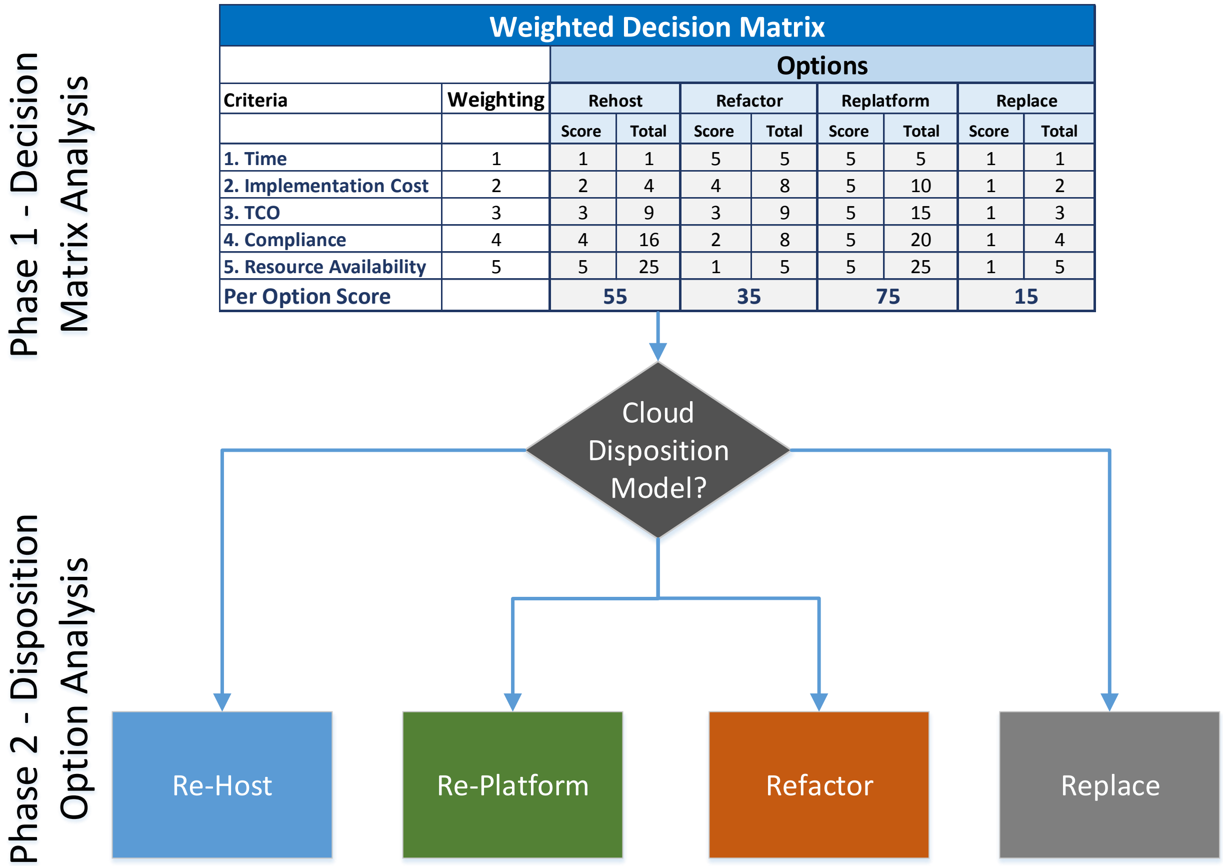
During the first phase your practitioners will work closely with the System Owner to develop decision a matrix that identifies evaluation criterion and assign weights for each. The recommendation is to identify a limited number of evaluation criteria (under 10) which should consist of essential drivers for the organization, i.e. external regulations, security requirements, budget, etc.

Next, weighting values are assigned to each criteria that are based on decisions about what the overall influence the criteria will have, one relative to the other, on the outcome (score). Different criteria could have the same or different relative weights assigned to them. For instance, in Table 7-2 Example Decision Matrix, Compliance is weighted more heavily relative to Time in influencing the total score.

Each application/workload will be scored by your practitioner together with Program or Product Sponsor, System Owner, SME's, System Admins, etc., based on complexity, across the four R's as shown. The weighted score for each option is determined by multiplying the assigned score by the weight assigned to this criteria. Table 7-2 provides a sample disposition analysis identifying Re-platforming as a preferred option:

Weighted Decision Matrix									
		Options							
Criteria	Weighting	Rehost		Refactor		Replatform		Replace	
		Score	Total	Score	Total	Score	Total	Score	Total
1. Time	1	1	1	5	5	5	5	1	1
2. Implementation Cost	2	2	4	4	8	5	10	1	2
3. TCO	3	3	9	3	9	5	15	1	3
4. Compliance	4	4	16	2	8	5	20	1	4
5. Resource Availability	5	5	25	1	5	5	25	1	5
Per Option Score		55		35		75		15	

Table 7-2 – Example Decision Matrix



Weighted Decision Matrix

		Options							
Criteria	Weighting	Rehost		Refactor		Replatform		Replace	
		Score	Total	Score	Total	Score	Total	Score	Total
1. Time	1	1	1	5	5	5	5	1	1
2. Implementation Cost	2	2	4	4	8	5	10	1	2
3. TCO	3	3	9	3	9	5	15	1	3
4. Compliance	4	4	16	2	8	5	20	1	4
5. Resource Availability	5	5	25	1	5	5	25	1	5
Per Option Score		55		35		75		15	

Phase 1 - Decision Matrix Analysis
Phase 2 - Disposition Option Analysis
Cloud Disposition Model?
Re-Host
Re-Platform
Refactor
Replace

Figure 7-1 – Application Disposition Decision Flow Overview

7.2.1 Re-Host Disposition

Figure 7-2 Re-host Disposition Decision Flow and the explanation that follows it describes in detail the analysis that would result in the use of Re-host disposition. NOTE: FISMA moderate or high classifications will drive vendor Government solution selection. Also, consider vendor affinity (i.e. Vendor 1 application to Vendor 1 CSP) and adapt the decision logic accordingly.

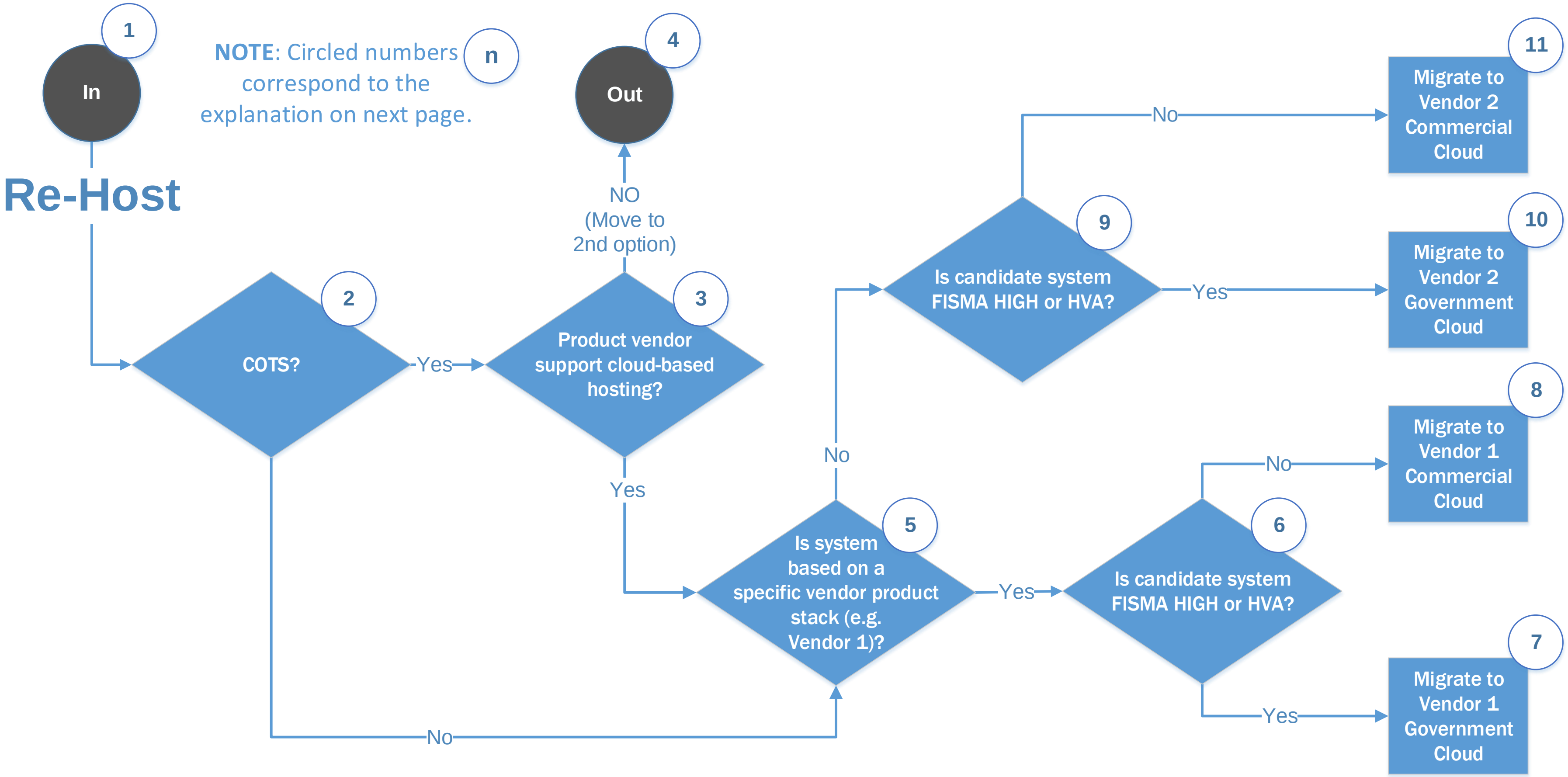

1
In
Re-Host
NOTE: Circled numbers correspond to the explanation on next page.
n
4
Out
NO (Move to 2nd option)
2
COTS?
Yes
No
3
Product vendor support cloud-based hosting?
Yes
5
Is system based on a specific vendor product stack (e.g. Vendor 1)?
No
Yes
9
Is candidate system FISMA HIGH or HVA?
No
Yes
6
Is candidate system FISMA HIGH or HVA?
No
Yes
11
Migrate to Vendor 2 Commercial Cloud
10
Migrate to Vendor 2 Government Cloud
8
Migrate to Vendor 1 Commercial Cloud
7
Migrate to Vendor 1 Government Cloud

Figure 7-2 – Re-host Disposition Decision Flow

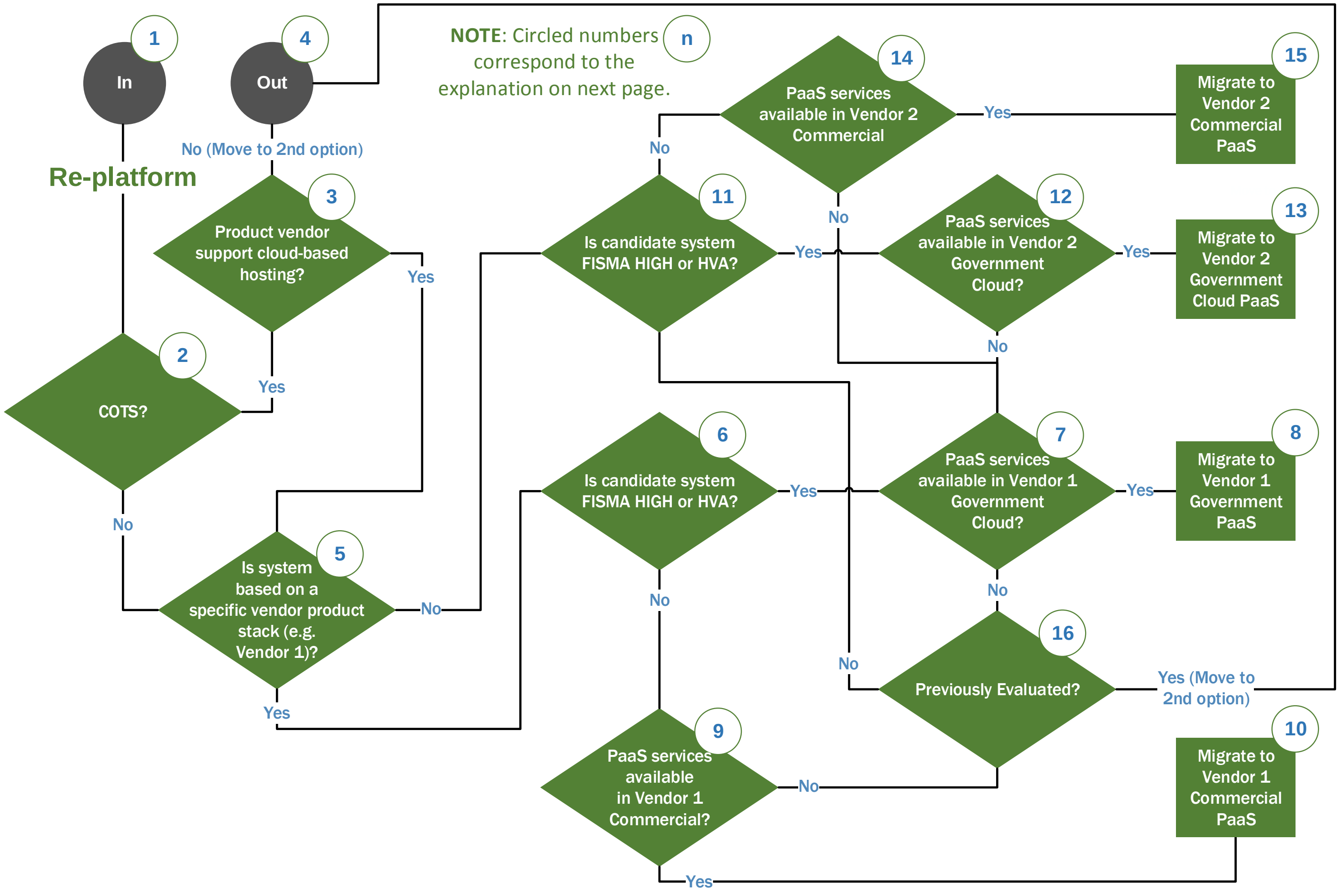
Re-host Decision Flow Description

1. Re-host option has been identified as part of the Phase 1 - Decision Matrix Analysis
2. Determine if the application is based on a COTS product.
3. If the application is based on the COTS product, determine if the product vendor will support cloud-based IaaS hosting.
4. If the vendor will not support cloud-based option, return to the second highest scoring option from Phase 1 - Decision Matrix Analysis. End of Re-hosting analysis.
5. If vendor will support the cloud-based hosting option or if application is not COTS based, determine if the application and the underlying stack is based on particular vendor products (e.g. Vendor 1, Vendor 2, etc.).
6. If the current application hosting solution is based on Vendor 1 product stack, determine if the application is rated as FISMA High and/or considered as a High Value Asset[2].
7. If the application is rated as FISMA High and/or considered as a High Value Asset, then it should be hosted in Vendor 1 Government Cloud IaaS.
8. If the application is not rated as FISMA High and/or considered as a High Value Asset, then it should be hosted in Vendor 1 Commercial Cloud IaaS.
9. If the current application hosting solution is not based on Vendor 1 product stack, determine if the application is rated as FISMA High and/or considered as a High Value Asset.
10. If the application is rated as FISMA High and/or considered as a High Value Asset, then it should be hosted in Vendor 2 Government Cloud IaaS.
11. If the application is not rated as FISMA High and/or considered as a High Value Asset, then it should be hosted in Vendor 2 Commercial Cloud IaaS.

[2] https://policy.cio.gov/hva/definition/

7.2.2 Re-Platform Disposition

Figure 7-3 Re-platform Disposition Decision Flow describes in detail the analysis that would result in the use of Re-platform disposition. NOTE: FISMA moderate or high classifications will drive vendor Government solution selection. Also, consider vendor affinity (i.e. Vendor 1 application to Vendor 1 CSP) and adapt the decision logic accordingly.



NOTE: Circled numbers n correspond to the explanation on next page.
1
In
4
Out
Re-platform
No (Move to 2nd option)
3
Product vendor support cloud-based hosting?
Yes
2
COTS?
Yes
No
5
Is system based on a specific vendor product stack (e.g. Vendor 1)?
No
Yes
14
PaaS services available in Vendor 2 Commercial
Yes
No
15
Migrate to Vendor 2 Commercial PaaS
No
11
Is candidate system FISMA HIGH or HVA?
Yes
12
PaaS services available in Vendor 2 Government Cloud?
Yes
No
13
Migrate to Vendor 2 Government Cloud PaaS
6
Is candidate system FISMA HIGH or HVA?
Yes
No
7
PaaS services available in Vendor 1 Government Cloud?
Yes
No
8
Migrate to Vendor 1 Government PaaS
16
Previously Evaluated?
No
Yes (Move to 2nd option)
9
PaaS services available in Vendor 1 Commercial?
No
Yes
10
Migrate to Vendor 1 Commercial PaaS

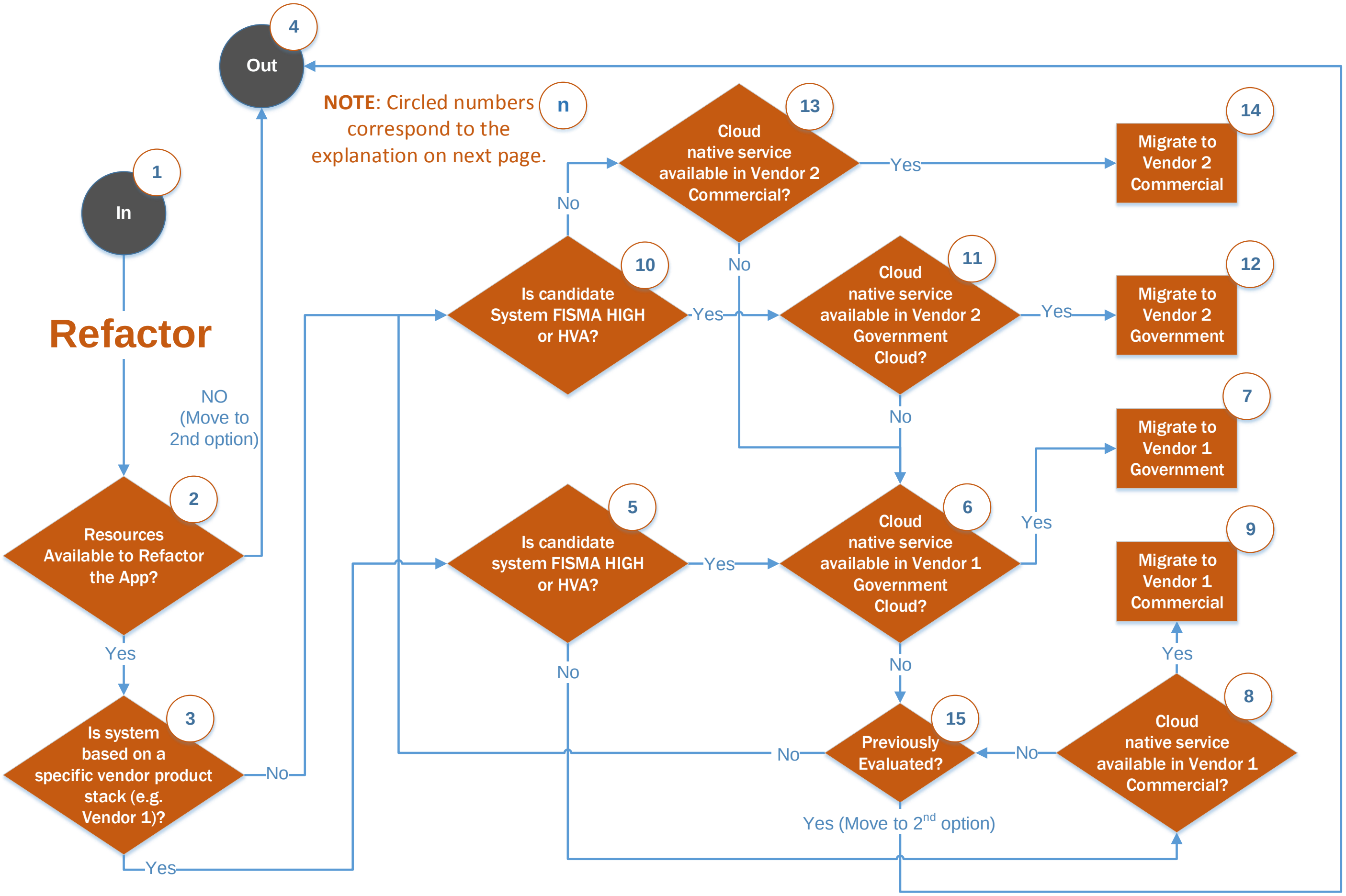
Figure 7-3 – Re-platform Disposition Decision Flow

Re-platform Decision Flow Description

1. Re-Platform option has been identified as part of the Phase 1 - Decision Matrix Analysis
2. Determine if the application is based on a COTS product.
3. If the application is based on the COTS product, determine if the product vendor will support cloud-based IaaS hosting.
4. If the vendor will not support cloud-based option or if this option has been evaluated previously, return to the second highest scoring option from Phase 1 - Decision Matrix Analysis. End of Re-Platforming analysis.
5. If vendor will support the cloud-based hosting option or if application is not COTS based, determine if the application and the underlying stack is based on particular vendor products (e.g. Vendor 1, Vendor 2, etc.).
6. If the current application hosting solution is based on Vendor 1 product stack, determine if the application is rated as FISMA High and/or considered as a High Value Asset.
7. If the application is rated as FISMA High and/or considered as a High Value Asset or if this service is not available in Vendor 2 Commercial Cloud or in Vendor 2 Government Cloud, determine if the candidate service is available in Vendor 1 Government Cloud.
8. If the PaaS service is available, then the application should be hosted in Vendor 1 Government cloud.
9. If the application is not rated as FISMA High and/or considered as a High Value Asset, determine if the candidate service is available in Vendor 1 Commercial Cloud.
10. If the PaaS service is available, then the application should be hosted in Vendor 1 Commercial cloud.
11. If the current application hosting solution is not based on Vendor 1 product stack or if this option has not been evaluated previously, determine if the application is rated as FISMA High and/or considered as a High Value Asset.
12. If the application is rated as FISMA High and/or considered as a High Value Asset, determine if the candidate service is available in Vendor 2 Government Cloud.
13. If the PaaS service is available, then the application should be hosted in Vendor 2 Government cloud.
14. If the application is not rated as FISMA High and/or considered as a High Value Asset, determine if the candidate service is available in Vendor 2 Commercial Cloud.
15. If the PaaS service is available, then the application should be hosted in Vendor 2 Commercial cloud.
16. If the PaaS service is not available in Vendor 1 Commercial Cloud or if is also not available in Vendor 1 Government Cloud, determine if this option has been evaluated previously.

7.2.3 Refactor Disposition

Figure 7-4 Refactor Disposition Decision Flow describes in detail the analysis that would result in the use of Refactor disposition. NOTE: FISMA moderate or high classifications will drive vendor Government solution selection. Also, consider vendor affinity (i.e. Vendor 1 application to Vendor 1 CSP) and adapt the decision logic accordingly.



Out
4
NOTE: Circled numbers correspond to the explanation on next page.
n
In
1
Refactor
NO (Move to 2nd option)
Resources Available to Refactor the App?
2
Yes
Is system based on a specific vendor product stack (e.g. Vendor 1)?
3
No
Yes
Is candidate System FISMA HIGH or HVA?
10
No
Yes
Cloud native service available in Vendor 2 Commercial?
13
Yes
No
Migrate to Vendor 2 Commercial
14
Cloud native service available in Vendor 2 Government Cloud?
11
Yes
No
Migrate to Vendor 2 Government
12
Migrate to Vendor 1 Government
7
Is candidate system FISMA HIGH or HVA?
5
Yes
No
Cloud native service available in Vendor 1 Government Cloud?
6
Yes
No
Migrate to Vendor 1 Commercial
9
Yes
Cloud native service available in Vendor 1 Commercial?
8
No
Previously Evaluated?
15
No
Yes (Move to 2nd option)

Figure 7-4 – Refactor Disposition Decision Flow

Refactor Decision Flow Description

1. Refactor option has been identified as part of the Phase 1 - Decision Matrix Analysis
2. Determine if the system owner has the available resources with the appropriate skills to support refactoring of the candidate application to be able to leverage cloud native capabilities.
3. If the system owner has the available resources to support application refactoring, determine if the current application hosting solution is not based on particular vendor products (e.g. Vendor 1, Vendor 2, etc.).
4. If the system owner does not have the available resources to support application refactoring or if this option has been evaluated previously, return to the second highest scoring option from Phase 1 - Decision Matrix Analysis. End of Refactoring analysis.
5. If the current application hosting solution is based on Vendor 1 product stack, determine if the application is rated as FISMA High and/or considered as a High Value Asset.
6. If the application is rated as FISMA High and/or considered as a High Value Asset or if this service is not available in Vendor 2 Commercial Cloud or Vendor 2 Government Cloud, determine if the cloud native capability is available in Vendor 1 Government Cloud.
7. If the cloud native capability is available, then the application should be refactored and hosted in Vendor 1 Government Cloud.
8. If the application is not rated as FISMA High and/or considered as a High Value Asset, determine if the cloud native capability is available in Vendor 2 Commercial Cloud.
9. If the cloud native capability is available, then the application should be refactored and hosted in Vendor 1 Commercial Cloud.
10. If the current application hosting solution is not based on Vendor 1 product stack or if this option has not been evaluated previously, determine if the application is rated as FISMA High and/or considered as a High Value Asset.
11. If the application is rated as FISMA High and/or considered as a High Value Asset, determine if the cloud native capability is available in Vendor 2 Government Cloud.
12. If the cloud native capability is available, then the application should be refactored and hosted in Vendor 2 Government Cloud.
13. If the application is not rated as FISMA High and/or considered as a High Value Asset, determine if the cloud native capability is available in Vendor 2 Commercial Cloud.
14. If the cloud native capability is available, then the application should be refactored and hosted in Vendor 2 Commercial Cloud.
15. If the cloud native capability is not available in Vendor 1 Commercial Cloud or in Vendor 1 Government Cloud, determine if this option has been evaluated previously.

7.2.4 Replace Disposition

Figure 7-5 Replace Disposition Decision Flow describes in detail the analysis that would result in the use of Replace disposition. NOTE: FISMA moderate or high classifications will drive vendor Government solution selection. Also, consider vendor affinity (i.e. Vendor 1 application to Vendor 1 CSP) and adapt the decision logic accordingly.

FedRAMP is preferred but not required. However, expect the approval process to be significant if not FedRAMPed.

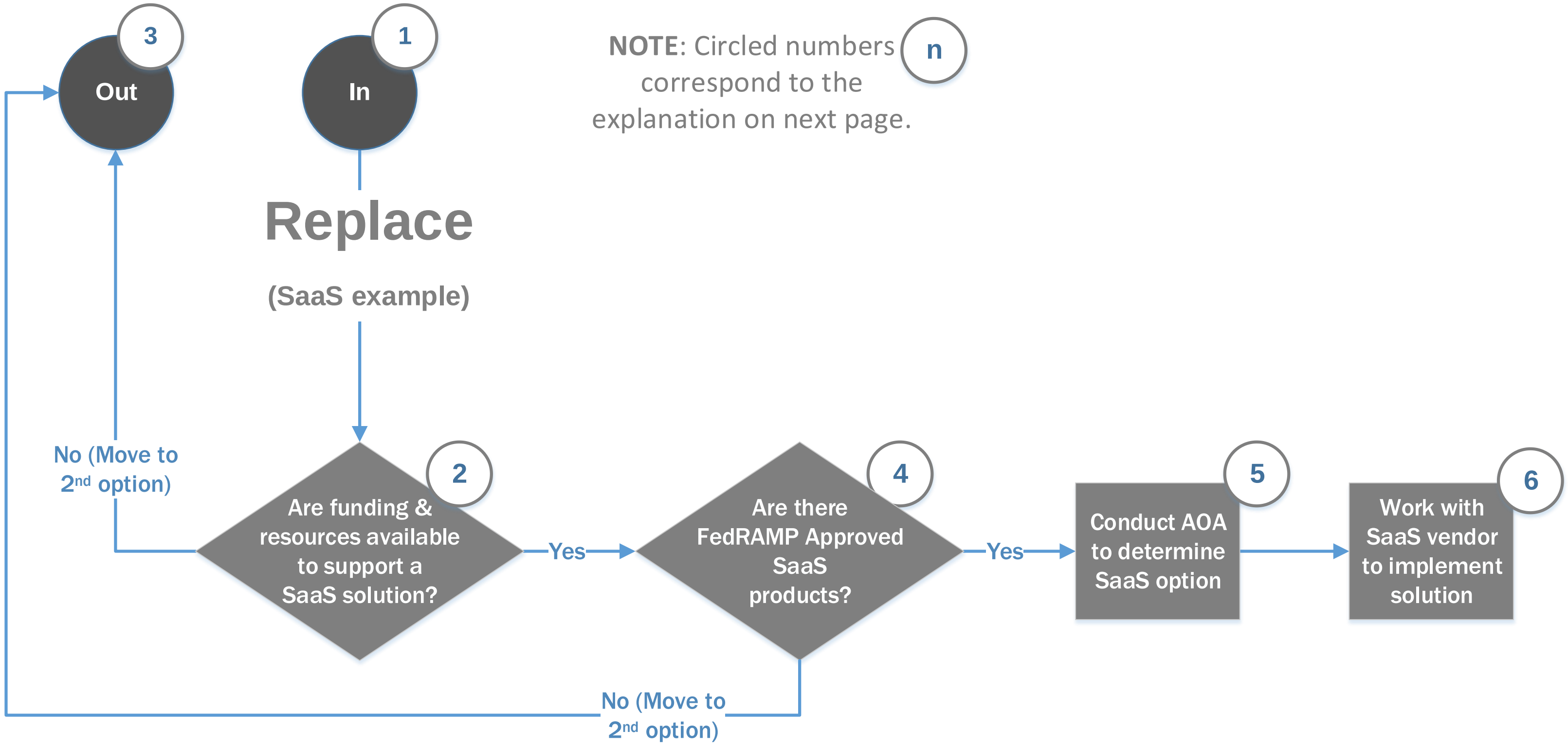

3
Out
1
In
NOTE: Circled numbers correspond to the explanation on next page.
n
Replace
(SaaS example)
No (Move to 2nd option)
2
Are funding & resources available to support a SaaS solution?
Yes
4
Are there FedRAMP Approved SaaS products?
Yes
5
Conduct AOA to determine SaaS option
6
Work with SaaS vendor to implement solution
No (Move to 2nd option)

Figure 7-5 – Replace Disposition Decision Flow

Replace Decision Flow Description

1. Replace for a SaaS option has been identified as part of the Phase 1 - Decision Matrix Analysis
2. Determine if the system owner has the available resources with the appropriate skills to support configuration of the SaaS solution.
3. If the system owner does not have the available resources to support SaaS implementation or if there are currently no FedRAMP authorized SaaS solutions, then return to the second highest scoring option from Phase 1 - Decision Matrix Analysis. End of Replace analysis.
4. If the system owner has the available resources with the appropriate skills to support configuration of the SaaS solution, then determine if there are FedRAMP authorized SaaS solutions and identify market leaders.
5. If there are FedRAMP authorized SaaS solutions, then conduct and Analysis of Alternatives (AOA) among leading solutions and determine leading SaaS product.
6. Upon completion of AOA, engage the SaaS CSP and commence implementation.

8 Cloud Deployment Model

8.1 Cloud Deployment Selection

The cloud deployment model utilizes application and workload attributes based on criteria to determine appropriateness of Private, Hybrid or Public cloud options.

There are three cloud deployment categories. Your practitioner will work with you to determine deployment model criteria specific to your goals. Some examples of criteria are given below.

In the various explanations in this Guide, on-premises is often referred to as the facility in which infrastructure is 'housed' – in an organization's data center or a co-location facility. For clarity, 'legacy' (non-cloud infrastructure) is used in the Guide to describe traditional on-premises data center facilities consisting of physical hardware, virtual machines, appliances, network, air, power, etc. As will be seen, this deployment model describes private and hybrid cloud with on-premises deployment options. Private cloud and hybrid cloud components can be housed in an organization's data center or co-location. The cloud deployment categories are:

8.1.1 Private Cloud

Private cloud is infrastructure that is implemented for exclusive use by a single organization (e.g. business unit, agency, department, etc.). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on- or off-premises.

Private cloud deployment may be a good choice for organizations that have very specific security or performance needs that may not be able to be met by the other deployment model types. They are a better choice in these circumstances than legacy data center infrastructure because cloud brings many benefits derived from modern technologies, automation, and DevSecOps.

Examples of Private cloud deployment selection criteria are:

- Other options may have been disqualified due to such circumstances as complexity of the application interdependencies (e.g. large shared DB's, middleware)
- The 'green' DCOI DC retention (on-premises) criteria such as power, air, etc. have been analyzed and the conclusion is that those criteria in combination with other drivers such as security, risk, data sensitivity, etc. justify Private cloud.

8.1.2 Public Cloud

Public cloud is infrastructure provisioned for use by the public, owned, managed and on the premises of the cloud provider. Examples are Amazon AWS, Microsoft Azure, Oracle Cloud, etc. CSPs.

Public cloud deployment may be a good choice for workloads that need to leverage cloud characteristics that are most effectively provided by public cloud service providers. Examples are vast resource pools, highly scalable rapid elasticity, large geographically diverse ecosystems, economies of scale, and measured service.

8.1.3 Hybrid Cloud

Hybrid cloud is the combination of distinct cloud infrastructures that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

Hybrid cloud deployment may be a good choice under certain circumstances. An example from a roadmap may call for is a composite of public cloud and on-premises interdependent workloads during cloud transformational periods.

CSPs offer transformational solutions. Your practitioners will work with you to plan strategies to leverage these opportunities.

Examples of Hybrid cloud deployment selection criteria are:

- The need for an option to migrate as many applications as practical to public cloud in the near term while still supporting dependent applications that aren't ready to migrate in a private cloud situation.
- An example solution for the above situation is the potential for use of a particular vendor as part of on-premises and hybrid strategy, which allows bridging deployments in public and private clouds during transition from on-premises to private, public or hybrid scenarios. Data and workloads are interoperable between private, public and hybrid in this case.

8.2 Cloud Service Model Selection

The cloud service model consists of three service types. Each service type is associated with one or more dispositions (i.e. the "5 R's"), depending upon the desired target state cloud architecture. One service type, along with one migration disposition, must be selected for each application or workload destined for the cloud. Cloud service types (relevant excerptions from NIST):

8.2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is the capability provided to the cloud consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

IaaS is typically utilized in the Re-host migration disposition scenario.

8.2.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) is the capability provided to the cloud consumer to deploy onto the cloud infrastructure consumer-created or acquired applications. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

PaaS is typically used where application Re-platform or Refactor is the migration disposition scenario

8.2.3 Software as a Service SaaS)

Software as a Service (SaaS) is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

SaaS by definition involves a third party application provider and therefore, the hosting model is up to the vendor (i.e. not DOE hosted or in DOE cloud). PaaS is preferred when possible over IaaS.

9 Workload Suitability & Placement

The potential of an application or workload perhaps not being suitable for cloud and needing to remain in an on-premises situation or possibly being a candidate for co-location placement is considered in this section.

Placement is analysis of applications and workloads to determine either their independence or the need to apply criteria that will logically group them for transformation and migration wave planning. This is referred to as *affinity grouping*.

For instance, it might be best to group multiple applications which heavily utilize the same database along with that DB in an affinity group. Applications that are tightly coupled such as through API's, web service calls, middleware, or are otherwise 'chatty' are other examples of workloads that are best analyzed in an affinity group. Analysis and planning in this way will help ensure functional and performance transformation objectives and operational continuity.

The appropriate destination CSP for an affinity group and the group migration wave planning in the Migration Roadmap phase of the CSP Delivery model is the output of Workload Suitability and Placement.

Figure 9-1 illustrates a Cloud Suitability and Placement use case including explanations of suitability rationale for selection of private, public or hybrid models, as well as placement affinities.

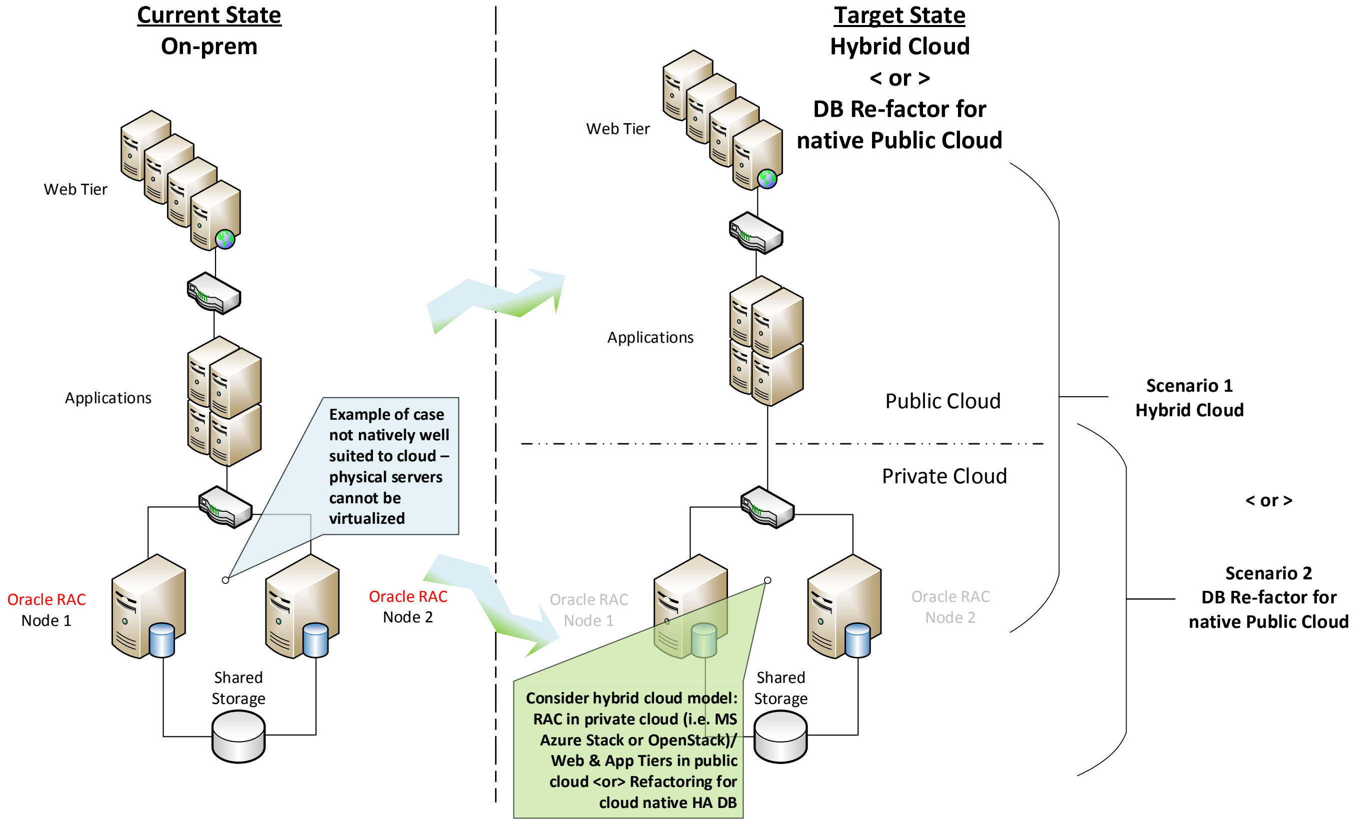

Current State
On-prem
Web Tier
Applications
Example of case not natively well suited to cloud – physical servers cannot be virtualized
Oracle RAC Node 1
Oracle RAC Node 2
Shared Storage
Target State
Hybrid Cloud
< or >
DB Re-factor for native Public Cloud
Web Tier
Applications
Public Cloud
Private Cloud
Oracle RAC Node 1
Oracle RAC Node 2
Shared Storage
Consider hybrid cloud model: RAC in private cloud (i.e. MS Azure Stack or OpenStack)/ Web & App Tiers in public cloud <or> Refactoring for cloud native HA DB
Scenario 1
Hybrid Cloud
< or >
Scenario 2
DB Re-factor for native Public Cloud

Figure 9-1 Workload Suitability & Placement Use Case

10 Business Case

The business case for cloud adoption consists of all the conventional elements of a business case, which is left outside the scope of this document. There are, however, specific elements applicable to cloud that are covered here with the recommendation that they not be overlooked.

The important ways in which we maximize cloud ROI are covered in Total Cost of Ownership (TCO) in this section.

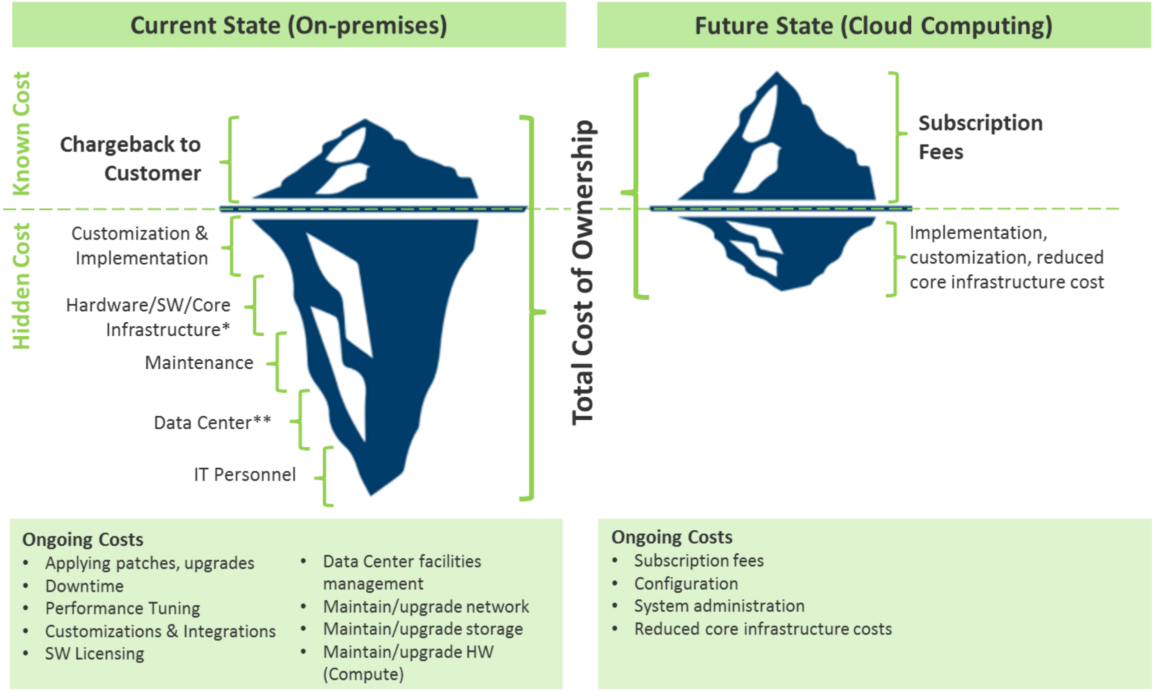
Cost models and other relevant financial considerations must be applied to candidate rationalization, disposition, deployment, suitability, and placement analysis outcomes.

Pay particular attention to transformational investment costs (application modernization, development, workforce preparation, etc.); as well as potential opportunity loss (e.g. cost premiums for remaining on-premises or support escalation costs, etc.).

10.1 Total Cost of Ownership (TCO)

There are several reasons why cloud could seem to be costlier than legacy on-premises or co-location hosting:

- Incorrect cloud implementation, e.g. legacy, tightly coupled, monolithic application(s) may have been hastily 'lift-and-shifted' (Re-hosted) into the cloud instead of being optimized to leverage appropriate cloud-native capabilities.
- Full Total Cost of Ownership (TCO) for legacy on-premises infrastructure may not be known resulting in the inability to compare legacy to cloud costs. As depicted in *Figure 10-1 – Total Cost of Ownership*, significant portions of the costs for legacy service components that make up TCO are probably not tracked or passed to the customer ('hidden costs').


Current State (On-premises)
Future State (Cloud Computing)
Known Cost
Hidden Cost
Chargeback to Customer
Customization & Implementation
Hardware/SW/Core Infrastructure*
Maintenance
Data Center**
IT Personnel
Total Cost of Ownership
Subscription Fees
Implementation, customization, reduced core infrastructure cost

Ongoing Costs

- Applying patches, upgrades
- Downtime
- Performance Tuning
- Customizations & Integrations
- SW Licensing
- Data Center facilities management
- Maintain/upgrade network
- Maintain/upgrade storage
- Maintain/upgrade HW (Compute)

Ongoing Costs

- Subscription fees
- Configuration
- System administration
- Reduced core infrastructure costs

**Core Infrastructure includes circuit costs, carrier costs, etc.*

***Data Center costs include building maintenance, heating/cooling, power, DCIM Tools, etc.*

Figure 10-1 – Total Cost of Ownership

How do we maximize cloud ROI? The following are well-founded:

- Minimized Capital Expenditures
- Pay-as-you-go for what you use (such as for on-demand elasticity). On-premises resources are typically grossly underutilized; averages of 10 to 20% are common.
- Managed services including logging, monitoring, analytics, Identity & Access Management, can reduce operational costs.

- Cost efficiencies of cloud native technologies and agile development methodologies such as DevSecOps and Continuous Integration/Continuous Development (CI/CD) are significant.
- Reduced Operations and Maintenance costs
- Energy savings (PUE on-premises ~2 vs. cloud ~1.1)**

** Source: *Lawrence Berkeley National Laboratory -The Energy Efficiency Potential of Cloud-Based Software: A U.S. Case Study, June 2013*

10.2 Cost Factors

Table 10-1 – Legacy & Cloud Cost Factors illustrates an approach to analysis and estimation of cloud costs for existing transformational workloads. It consists of two legacy cost factor that are probably most relevant to cloud cost estimation – compute utilization and compute class (vCPU/memory). The other six factors are to be estimated by practitioners based on available or derived workload requirements and experience.

The red/yellow/green heat map application to the Estimate Opportunity element is simply to convey a sense of the degree of confidence that is likely in the estimate. Combined with the high, medium or low impact expectation, the practitioner will gain insight into how to use cost model data for planning purposes.

For example, *legacy compute percentage utilization over* time is usually unknown (therefore, red). But the impact of not knowing this factor as input to the cloud cost model is high. Therefore, if a basis for the Estimate Opportunity is known or can be obtained, especially for factors combined with high or medium impacts, the resulting confidence in cost estimation will be improved.

The practical application of this approach is demonstrated in *Appendix 2 OneID Cost Factors Case Study*.

Important Note: special attention is drawn to the last cost factor – Unknown Total Cost of Ownership (TCO). It's visibility in cloud is profound compared to the typical legacy bill-back or show-back situation.

Legacy or Cloud Cost Factor	Estimate Opportunity	Impact	Comments
Legacy Compute Percentage Utilization over time	Usually unknown	H	Legacy compute utilization can be used as a rough approximation for right-sizing cloud instances. It is the basis for determination of whether to factor cloud cost of on-demand or reserved compute instances.
Compute Class	Usually known or can be obtained	M	A function of virtualization. Legacy [(# cores or vCPU) + memory]
Bring Your Own Licenses (e.g. COTS or DB; OS to PaaS; etc.)	Integral to cloud architecture decisions	H	Bring your own license (BYOL) means utilizing licenses in the cloud that you already own (if permissible). Examples are Commercial Off The Shelf (COTS) applications or database; or an OS to PaaS; etc. BYOL cost must be added to the output cost of the CSP cost calculator. For any CSP-provided licensing, it must be factored into the CSP cost calculator. A combination of BYOL and CSP-provided is valid.
Cloud Subscription Term and up front commitments as factors of discount(s)	Selectable in cloud cost model	M	The length of cloud subscription term and up front "down payment" can dramatically impact total cost of ownership (TCO). The practitioner will select options in the model for optimized cost estimation.
Storage Volume Type and IOPS	Usually known or can be obtained	M	Apply best practices allocation and tier selection
Cloud Data Transfer volumes: cloud Egress	Usually unknown	H	Can be a significant monthly cloud cost estimation confidence limitation if unknown.
Dual Region COOP/availability, replication	Cloud value add	M	Potential DR, high availability and automated replication cloud value proposition
Other – Unknown Total Cost of Ownership (TCO)	Usually unknown	H	Hidden or lump sum costs that may be billed as apportioned cost in legacy but will be easily attributable (visible) in cloud. Refer to Figure 10-1 – Total Cost of Ownership.

Table 10-1 -- Legacy & Cloud Cost Factors

10.3 CSP Cost Calculators: What to Look Out For

Potential cost avoidance (routine Capital Expenditure outlays, infrastructure refreshes, overbuild requirements to meet short-lived instantaneous demands, to name a few) is a primary motivator for cloud adoption. The usual assumption is that migration of on-premises hosting to cloud will result in cost savings. In reality, a jump into cloud without adequate transformational strategy often results in higher initial cloud costs and the inability to realize some inherent added values of cloud.

As an implication example and mitigating strategy, detailed guidance for the following cost situation is provided in this guide. Monthly data transfer volumes out of cloud (egress) is perhaps the most common unknown cloud cost factor.

While Cloud Service Providers (CSP's, e.g. Amazon AWS, Microsoft Azure) calculators accept such estimates as variables, there is usually no basis for actual data volumes in the legacy state on-premises architectures. Only a study of the target state cloud architecture and interconnectivity and communications of on-premises and cloud interdependent applications can lead to estimates of cloud egress data volume. Due to the nature of how CSP's structure their cost models, egress data volume can be a significant 'hidden' monthly cloud cost. Strategies to fully explore refactoring opportunities and to accurately estimate cloud Total Cost of Ownership (TCO) are highly recommended.

11 Additional Guiding Principles for Cloud Implementation

The following is a collection of additional best practice and applied guiding principles for cloud migration. There are a number of key differences between traditional on-premises and cloud computing environments.

11.1 Key Cloud Architecture & Design Considerations

The architecture, design and implementation for Re-host and Refactor application dispositions, as well as new or cloud native applications, will be influenced by cloud operating characteristics. DevSecOps processes are applicable in different degrees to the following.

- Re-hosted (often referred to as "lift-and-shift") applications maintain their existing operating model. However, they should be analyzed for the potential to leverage the ability to manage infrastructure as code through API's. You may find this aids in repeatable build processes and improvements in reliability.
- Refactored applications leverage automation and supporting cloud services such as auto scaling and self-healing architectures.
- The architecture and design for new applications implemented in cloud or cloud native applications should be fully automated utilizing DevSecOps processes.

Each of the following baseline set of factors should be considered when creating the cloud design.

- Scalability
    - Growth without performance penalties
    - On-demand resources
    - Economies of scale leverage business value from ecosystem
- Naming and tagging standards
- Automation
    - Instantiation of cloud resources is to be automated and repeatable
    - Cloud Product Services Catalog and Self-Provisioning
    - Auto Scaling
    - Auto-recovery
- Availability
- High Availability & Fault Tolerance
- Continuity of Operations (COOP) and Disaster Recovery
- Data Replication & Backups Strategy
- Federal Records Management
- Standardized Policies & Procedures
    - Security
    - Authentication
    - Monitoring & Controls
    - Licensing
    - Patching

11.2 Common Operations for Cloud

11.2.1 Governance

Cloud governance is focused on skills and processes that align IT strategy and goals with you organization's mission strategy and goals. It's assurance that the mission value of the IT investment is maximized, while mission risks are minimized.

The core governance capabilities should be:

- Portfolio Management
    - Discover and catalog (e.g. CMDB) mission functional capabilities served by IT systems and the applications that deliver those capabilities
    - Determine cloud eligible workloads for migration
    - Prioritize IT investments, programs and projects aligned with your cloud adoption mission goals
- Change Management
    - Define and implement rigorous policies and processes for change control
- Release management
    - There are opportunities in cloud adoption to leverage Continuous Integration/Continuous Development (CI/CD) techniques to manage releases and rollbacks in expeditious and efficient ways.
- Policies and Administration
    - DevSecOps
    - Cloud on-boarding including criteria and adaptive procedures
    - Policies pertaining to environments (e.g. Sandbox, Dev, Test, Production): appropriate use, deployments, degrees of isolation, code promotion policies, etc.
- Mission IT Performance Measurement
    - Measure and optimize processes in support of your mission's goals
    - Develop new skills and processes to leverage cloud-centric Key Performance Indicators (KPIs)
    - Create processes to ensure cloud consumption and mission outcomes seen in KPIs are consistent with your mission goals; adjust as necessary
- License Management
    - Procure and manage distribution, use and costs of licenses for software and services
    - Optimize the use of cloud native and bring-your-own license options (i.e. cost implication)

11.2.2 Security

Leveraging the cloud provider's investments in cyber security and network protection allows DOE to focus on its own security efforts rather than investing heavily in maintaining a base capability. It is recommended that FedRAMP Joint Authorization Board (JAB) certifications be used for selecting cloud providers. The FedRAMP program provides a standardized approach to the assessment, evaluation, authorization, and continuous monitoring of cloud products and services.

DOE can focus on controls and monitoring procedures that are directly applicable to its requirements. Look at any previously completed cloud authorization to reuse whatever is applicable wherever possible. This approach produces a "do once, use many times" work template that greatly reduces labor costs associated with achieving an enterprise ATO applicable to that particular CSP's cloud environments.

Select and implement security controls that meet your organization's objectives for visibility, auditability, control, and agility. Properly implemented in cloud, the requirements of the most security-sensitive organizations can be met.

- Identity & Access Management Policies & Governance -- create access control mechanisms and manage the permissions for each. Privileges must be granted on a least privileged basis (typically roles-based) for users to provision and orchestrate resources.
- Detective Control -- provide a robust security posture by correlating logs from cloud services with event generation from applications, operating systems, databases, etc. Implement centralized logging and monitoring solutions for visibility in near real time for comprehensive visibility.
- Data Protection -- addresses the capability for maintaining visibility and control over data, and how it is accessed and used in the organization.

11.2.3 Incident Response

Incident response is the ability to manage response, harm reduction, and normal operations restoration throughout a security incident. There are inherent cloud services as well as other vendor tools that can be integrated for these purposes.

11.2.4 Service Level & Operational Level Agreement

Service Level Agreements (SLA) and/or Operational Level Agreements (OLA) [often in a Memorandum of Understanding (MOU)] define operations life-cycles to enable, run, operate and recover IT workloads to levels that are agreed upon by IT and Mission stakeholders. SLAs typically include elements of application and service monitoring, reporting and analytics, and continuity of operations and disaster recovery. Agreements define criteria for conformance with your organization's service needs. Cloud offers Operations new features and greater visibility into their compliance with agreements.

11.3 Workforce & Re-skilling

Similar to the evolution of the traditional IT services from the on-premises to cloud based model, the role of the IT support staff will also have to evolve to support the cloud operations. As depicted in Figure 11-1, the IT support staff will have to transition from being a specialist in a particular area to a multifaceted IT professional responsible for cloud operations support such as networking, system administration, backup, recovery, performance monitoring, SLA management, etc.

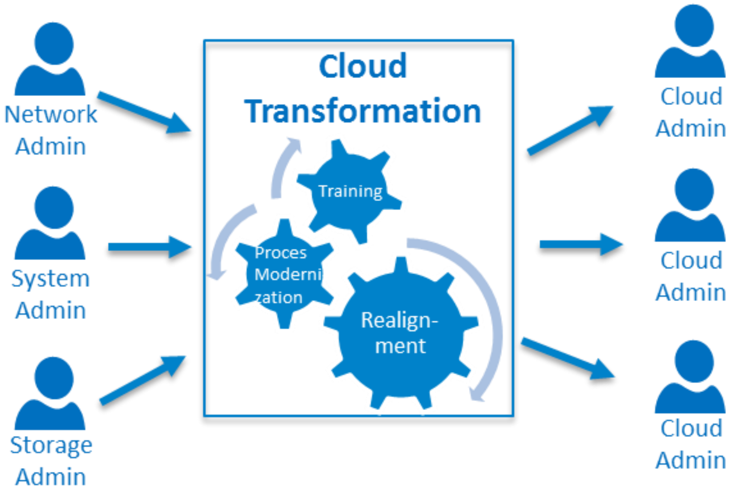


Figure 11-1

During transition from the on-premises hosting model, which offered limited automation opportunities, to the cloud operating model the emphasis will have to shift from manual processes (e.g. installation and configuration) to automating (scripting) configuration of the entire stack (Infrastructure as Code). As part of the skills development effort the organization will have to conduct a comprehensive skills assessment in order to measure level of experience and skills around the cloud technologies below:

- IaaS (compute, storage, networking, etc.)
- PaaS
- Containerization (e.g. Docker)
- Scripting /coding (e.g. Python, Power Shell, Node.js, etc.)
- Continuous Integration (CI)/Continuous Delivery (CD) tools (Git, Jenkins, CodeDeploy, CodePipeline, etc.)
- Automation tools (Chef, Ansible, CloudFormation, TerraForm, etc.)

The assessment results will have to be analyzed to determine gaps and to develop a training plan that will help to ensure operational readiness aligned with cloud adoption milestones defined in Section 6.6 – Migration Roadmap. When executing training, practitioners will identify vendor/industry training materials and will help to tailor them to DOE-specific requirements if necessary. Practitioners will also have to work closely with the Operations leadership to identify training cohorts and to define milestones (i.e. certification completion deadlines). Training will have to be delivered via the following:

- Online labs/workshops
- Classroom based training
- Internal workshops

- Hands-on practice

11.4 IT Service Catalog

This is IT's capability to define, catalog, offer for selection, advertise, deliver, and otherwise maintain sets of IT services and SLA's. It enables consistently provisioning service patterns that are fundamental to cloud.

11.5 Environments: Development, Test & Production

When developing an enterprise cloud capability it is recommended to stand up a Development/Test (Dev/Test) Environment completely separate from Production. The Dev/Test environment should be configured as a separate tenant and should have its own set of dedicated core infrastructure resources (i.e. Firewalls, AD, compliance/monitoring tools, etc.). Having completely separate core infrastructure will allow the cloud team to conduct tests and pilot efforts without having any potential impact on production operations. Additional environments such as sandbox, staging, QA/UAT and performance test may be appropriate for certain requirements.

11.6 Load Balancing, Failover & High Availability

When defining a cloud hosting specification for a particular system, working closely with the system owner to define high availability (HA) and disaster recovery (DR) implementation approach will be needed. As part of this effort, it is important to consider the system availability requirements and the extent of the data loss the system owner can tolerate. System availability is the percentage of time that the system will work as required when required during the period of the mission. Example of HA requirement is 99.999% or Five-9's, which means that system will not be operating correctly less than 5 minutes during a given year. Data loss tolerances are defined as recovery time objective (RTO) and recovery point objective (RPO). Understanding the impact and tolerance for downtime will help drive the decisions that need to be understood in order to properly design the architecture and the level of complexity and cost required to support disaster recovery. The RTO and RPO requirements could be met by implementing the appropriate level of compute and storage redundancy, leveraging intra/inter-region replication, global/local load balancing, and other CSP-specific or 3rd party HA/DR solutions.

11.7 Portability and Exit Strategies

A recommendation is, from the start of and throughout planning, to architect cloud solutions with an exit or portability strategy in mind (option to switch from one CSP to another or to/from hybrid cloud). If something unforeseen reduces an application's suitability for a particular CSP, or cloud viability, a change can be executed to alleviate the problem.

Refer also to Section 8.1.3 Hybrid Cloud

- Support of open source technologies in cloud give you alternatives to CSP-proprietary tools, enabling a switch to another CSP.
- A range of industry standard solutions allow you options to architect for application and data interoperability from the beginning of your cloud journey.
- Even if you have workloads operational in the cloud which are less than optimally architected and experience issues, there are options to export data and virtual machines or images.
- Another exit (or re-implementation) example might be a prior choice to re-host a workload rather than refactor when it could have benefitted from that strategy.

It is important to understand from CSPs vendors up front the portability and exit options they support.

11.8 DevSecOps

It is highly recommended that planning and execution of strategies for shift to DevSecOps using agile methodologies be undertaken, consisting of:

- Continual collaboration between information security, application development, and IT operations teams. Having all three teams immersed in all development and deployment activities makes it easier for the information security team to integrate controls into the deployment pipeline without causing delays or creating issues by implementing security controls after systems are already running (helps facilitate incremental ATO approval process).
- Technical phases of projects supported by common tools and automation processes, collaboration replaces handoffs, codebase/IT infrastructure is agile and functional by default; Security team is involved in the automation process and helps map security controls to build automation capabilities.
- Eliminate the complexity of human intervention and replace with repeatable, standardized pipelines for infrastructure deployments; enable infrastructure self-provisioning for application teams.

11.8.1 DevSecOps Baseline Process

The baseline DevSecOps process includes four major focus areas:

- Build - Build automation code for Infrastructure-as-a-Service (IaaS) and Platform-as-a-service (PaaS) offerings to facilitate provisioning of infrastructure and platforms in cloud environment. Also build application code in Ansible playbook for deployment and establish a consistent delivery process.
- Test - Continuous Integration (CI) is performed when the code commits to GitHub or CircleCI, committed code is pulled, unit and integration tests are run, and notification is sent to deployment teams.
- Deploy - Use a deployment dashboard to select the latest code build. Application code is deployed to the target environment (Dev/Test/Prod) in cloud.
- Operations - The standard process for streamlined operations should be established using the following recommended approach:
    - Establish approved baseline vendor images, built and deployed in the environment for the OS.
    - Utilize appropriate security tools like ClamAV (Anti-Virus), Nessus (for security scanning and compliance checking), and OSSEC (for Host Intrusion Detection System, HIDS).
    - Implement tools like SolarWinds, Splunk, CloudWatch to establish standard monitoring and notification methods.
    - Utilize syslog for centralized logging of system logs, application logs, and tool logs.

11.8.2 Development Approach

The application migration team should plan to deploy (migrate) their respective application(s) to a Test/Stage environment in the cloud environment first. This will allow the application team to test their application for functionality, performance, and scalability in the cloud. This will also allow the security team to access the applications and the corresponding infrastructure platform (for Security Groups, Network ACL (NACL), OS images, and subnet/VPC configurations) and map these to appropriate security controls for ATO certification. The migration team can then take the findings from the initial security assessment and make sure the gaps are addressed before the application(s) are deployed in the production environment. Additionally, this will enable faster turnaround time to acquire the final system ATO certification in the cloud. In this way, the Security team works hand-in-hand with Development in the cloud transformation and migration efforts, streamlining the overall process.

11.8.3 Security Assessment and Authorization Process

As part of the post migration and pre-operations phase, security control requirements need to be met. It is recommended to coordinate with the security office to come to a mutual agreement on how to successfully meet security requirements for your migration project.

11.8.4 Assessment Approach

The ATO (or A&A) process requires the documentation of a System Security Plan (SSP), review and approval of the system security architecture, and assessment of the security controls. These tasks are typically performed after the pre-identified and agreed upon security boundary for the migration project has been defined. However, as a means to expedite the process, incremental migration component level authorizations may be granted while final authorization is being achieved, and assuring that all security requirements are fully met. This may be the approach to take for large migration initiatives where distinct components or applications make up the overall scope (e.g. CMS and database, analytics software and database, document repository and database).

The premise of this approach is that the Security Operations and Security Engineering teams would be engaged to perform incremental reviews and approval of documentation and controls, as well as incremental scans (e.g. scans of OS baseline images and mitigation of high or critical findings performed first along with individual application scans as they are deployed to the Production environment). This is made possible with an established dedicated cross-functional teaming structure established along with an agile scrum development methodology. The migration application and security teams will need to closely coordinate on control assessment and document review schedules. The application team will usually take the responsibility of tracking the progress of both areas.

11.8.5 Roles & Responsibilities and Teams Involved

Many teams are involved in a migration project. Below is a synopsis of the roles some of the teams may play.

- Enterprise Architects and Cloud Subject Matter Experts (SMEs) will participate in the following:
    - Enterprise Architects will incorporate cloud principles into the enterprise architecture.
    - Enterprise Architects will build cloud reference architectures and develop repeatable processes that facilitate cloud adoption and strategies.
    - Practitioners fulfill a cloud leadership role to meld the organizational structure with the cloud suitable operational efficiencies.
    - Enterprise Architects and Cloud SMEs will stay ahead of the cloud technology curve and aid in organizational cloud adoption and maturity.
    - Cloud Governance: Develop Cloud standards and policies, and perform transformative services to support agile based cloud adoption.
- Project Sponsor: The Project Sponsor serves as the person who is held accountable for the migration effort. They are also the ones responsible for procuring the funding and ensuring the cloud migration project(s) remains a viable proposition and its benefits are recognized.
- Project Team: The core business team that serves as the decision makers on day to day migration activities and is responsible for ensuring the expectations of the Project Sponsor and the customer are managed appropriately.
- Migration Team (DevSecOps team)**:** A cross functional team of developers and security engineers that serve as the primary technical POCs for the migration. This team provides knowledge regarding the current environment(s), as well as the resources for the actual migration.
- Security Team (Policy, Compliance and Engineering): Security provides resources to ensure the environments, applications, and tools that are deployed are complete and can be approved for Authorization To Operate (ATO). This team serves as the primary POCs for authorization policy and engineering guidance and will coordinate with the migration team on security controls assessment, documentation review, and approval.
- Scrum Master: The day to day facilitator who ensures the team follows an agile development process. The Scrum Master is responsible for ensuring impediments are removed, appropriate issues are escalated, and the team stays focused and on track.
- Scrum Team: Includes the Project Team, Migration Team, Security, and the Scrum Master.

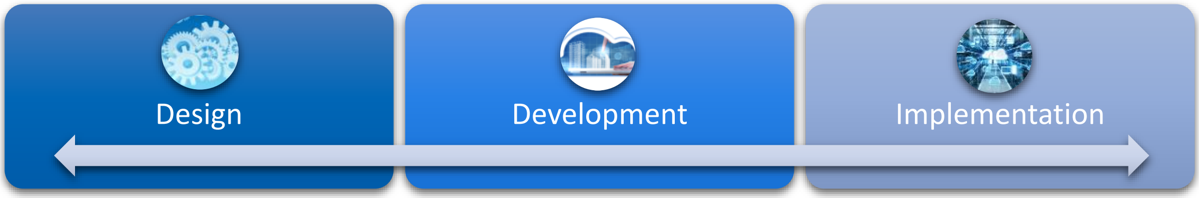
11.9 Federal Records Management

Federal laws and regulations require agencies make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency. They provide that systematic attention be given to records from creation to disposition, and for records preservation where applicable, to ensure public accountability, to protect the history of the Government and to safeguard the legal and financial rights of the Government and the public. They also require agencies ensure adequate information to conduct business under other than normal operating conditions and to resume normal business afterwards.

11.9.1 Design, Development and Implementation

Records management and preservation considerations must be incorporated into the design, the development and the implementation of cloud solutions. The capital planning and systems development life cycle processes for the same must ensure:

- Records management controls are planned and implemented.
- Records in the cloud will be retrievable and usable for as long as needed to conduct agency business (i.e., for their NARA-approved retention period).
- Transfers of permanent records from the cloud to NARA are in accordance applicable regulations.
- Provisions of a standard interchange format (e.g., ASCII or XML) when needed to permit the exchange of electronic documents between offices using different software or operating systems.



11.9.2 Records Management Controls

Controls are necessary to ensure Federal records in the cloud provide adequate and proper documentation of agency business throughout the records lifecycle. The controls include:

- Reliability to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
- Authenticity to protect against unauthorized addition, deletion, alteration, use, and concealment.
- Integrity, such as audit trails, to ensure records are complete and unaltered.
- Usability mechanisms to ensure records can be located, retrieved, presented, and interpreted.
- Content mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.
- Context mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.
- Structure to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

11.9.3 Essential Records

Essential records are records needed to support continuation of DOE's essential functions during emergencies and/or disasters, and/or to protect the legal and financial rights of the Government and those affected by DOE activities. Agencies' retrieval procedures for essential records hosted in the cloud must be easily implemented to support continuity operations and user needs. The appropriate hardware, software and system documentation must adequately operate the system to protect the essential records and ensure appropriate and timely access during emergencies and disasters, as well as effective dispositioning to support cycling/removal of cancelled, expired and superseded essential records.

12 Summary

There have been many best practices and experienced-based guiding principles detailed in this guide which will help decision makers be smart about cloud adoption, planning and implementation. Most are generic and can be applied to any CSP.

Each CSP is unique of course, with its own products, services, eco-systems, and complexities. It may be helpful to review candidate CSP documentation and the respective vendor resources (i.e. websites, guides, etc.).

Cloud Implementation Guiding Principles Checklist

Here is a summary of the guiding principles for making your cloud adoption successful.

Guiding Principle	Reference Section
The IT organization must orient itself toward delivery of innovative, business-focused services and capabilities. Without this strategic evolution, the process of designing, building, and operating advanced, integrated, and effective systems is exceedingly difficult.	1
Of extreme importance is the recognition that a jump into cloud without adequate transformational strategy often results in higher initial cloud costs and the inability to realize some inherent added values of cloud.	1
Enterprise Architecture should provide the guardrails (governance, policies and standards) for cloud adoption and migration.	1
It is recommended that cloud practitioners guide the use of cloud adoption to help you achieve success and to reduce the risk of cloud exit or 're-implementation' issues.	4
Transformation involves shifts in IT and mission value assessment, analysis, technologies, architecture, development, operations, personnel skills, and end-to-end enterprise processes.	1
Without adequate consideration of the implications of proper strategies for modernization and transformation of legacy analysis, development, operations planning and processes, a jump into cloud can be highly impactful with potentially unintended consequences.	4
Due to the nature of how CSP's structure their cost models, egress data volume can be a significant 'hidden' monthly cloud cost. Strategies to fully explore refactoring opportunities and to accurately estimate cloud Total Cost of Ownership (TCO) are highly recommended.	4

Guiding Principle	Reference Section
It is highly recommended that planning and execution of strategies shift to DevSecOps using agile methodologies. There are best-practice opportunity to transform to DevSecOps agile sprints that drive a high degree of collaboration between Development, Cyber Security and Operations for continuous development.	4
This reference guide encourages a more risk-based approach to cloud adoption and integration, securing systems that place appropriate emphasis on continuous data-level protections and awareness, and that fully leverage modern virtualized technologies. Additionally, it is critical that agencies have comprehensive visibility of their data, both on-premises and in the cloud, and perform continuous monitoring in order to detect malicious activity.	4
The various models throughout the guide consist of best practice components for establishing cloud migration strategy and achieving practical implementation.	4
There are cloud-specific business case elements applicable to cloud that are covered here with the recommendation that they not be overlooked. Pay particular attention to transformational investment costs (application modernization, development, workforce preparation, etc.); as well as potential opportunity loss (e.g. cost premiums for remaining on-premises or support escalation costs, etc.).	10
Full Total Cost of Ownership (TCO) for legacy on-premises infrastructure may not be known resulting in the inability to compare legacy to cloud costs.	10
Special attention is drawn to the last cost factor – Unknown Total Cost of Ownership (TCO). It's visibility in cloud is profound compared to the typical legacy bill-back or show-back situation.	10
A jump into cloud without adequate transformational strategy often results in higher initial cloud costs and the inability to realize some inherent added values of cloud.	10
Monthly data transfer volumes out of cloud (egress) is perhaps the most common unknown cloud cost factor. While Cloud Service Providers (CSP's, e.g. Amazon AWS, Microsoft Azure) calculators accept such estimates as variables, there is usually no basis for actual data volumes in the legacy state on-premises architectures. Only a study of the target state cloud architecture and interconnectivity and communications of on-premises and cloud interdependent applications can lead to estimates of cloud egress data volume. Due to the nature of how CSP's structure their cost models, egress data volume can be a significant 'hidden' monthly cloud cost.	10

Guiding Principle	Reference Section
Strategies to fully explore refactoring opportunities and to accurately estimate cloud Total Cost of Ownership (TCO) are highly recommended.	10
The architecture and design for new applications implemented in cloud or cloud native applications should be fully automated utilizing DevSecOps processes.	11.1
Cloud governance is focused on skills and processes that align IT strategy and goals with you organization's mission strategy and goals. It's assurance that the mission value of the IT investment is maximized, while mission risks are minimized.	11.2.1
Select and implement security controls that meet your organization's objectives for visibility, auditability, control, and agility.	11.2.2
Utilize FedRAMP Joint Authorization Board (JAB) certifications for selecting cloud providers. The FedRAMP program provides a standardized approach to the assessment, evaluation, authorization, and continuous monitoring of cloud products and services. DOE can focus on controls and monitoring procedures that are directly applicable to its requirements. This approach produces a "do once, use many times" work template that greatly reduces labor costs associated with achieving an enterprise ATO applicable to that particular CSP's cloud environments.	11.2.2
The role of the IT support staff will also have to evolve to support the cloud operations.	11.3
When developing an enterprise cloud capability it is recommended to stand up a Development/Test (Dev/Test) Environment completely separate from production.	11.5
A recommendation is, from the start of and throughout planning, to architect cloud solutions with an exit or portability strategy in mind. The strategy can be invoked if something unforeseen reduces an application's suitability for a particular CSP, or cloud viability. Refer also to Section 8.1.3 Hybrid Cloud.	11.7
Make use of the range of industry standard solutions allow you options to architect for application and data interoperability from the beginning of your cloud journey.	11.7
It is highly recommended that planning and execution of strategies for shift to DevSecOps using agile methodologies be undertaken.	11.8
The Federal Records Act – the management of federal records in electronic systems, to include cloud services, requires electronic systems to manage federal records in electronic format. Refer to the section for requirements.	11.9

Guiding Principle	Reference Section
Know your data – what and how much?	Appendix 2

13 Acknowledgements

The Department of Energy, Office of the Chief Information Officer, the Office of the Deputy CIO - Architecture, Engineering, Technology & Innovation, and the Enterprise Architecture Governance Board would like to acknowledge the following contributors and editors. The work of these and many others working in the background have shaped this guide to be a resource for the Department. It is the hope that this guide will be a resource for organizations here at DOE and beyond to assist in strategizing, planning and implementing successful migrations to the cloud. Thank you!

Contributors	
Max Everett, CIO Pamela Isom, DCIO Architecture Engineering Technology and Innovation (IM-50), DOE Chief Data Officer, EAGB Co-Chair Jeanne Beard, Office of Emergency Management and EAGB Co-Chair Barb Helland, Office of Science, EAGB Bryan Long, Acting Principal Deputy CIO	Executive Sponsorship
Enterprise Architecture Governance Board	All
Alberto Alverez	OCIO, Policy and Governance Office
Kenneth Calabrese	OCIO, IM-50, Chief Data Office, ARB Co-Chair
Maria Levesque	OCIO, Chief Privacy Office
James Knollman	OCIO, IM-50, Chief Data Office
Jonathan Arlotti-Parish	NNSA, ARB Co-Chair
Igor Pedan	Energy Information Administration
Steven Tibrea	CIO, Savanna River National Laboratory
David Tucker	Enterprise Architect, WAPA
Shannon Hughes	OCIO, Chief Information Security Office
Antonio Sandoval	OCIO, IM-50, Chief Data Office
Edward Siewick	OCIO, Chief Information Security Office
Greg Sisson	OCIO, Chief Information Security Office
William Stone	OCIO, Policy and Governance Office
Pacific Northwest National Laboratory	Numerous contributors
Other	

Appendix 1 – AWS Solution Architecture Example

Note: the CSP in the following is for example purposes only; the illustration is intended to be vendor-agnostic.

Appendix 1-1 is a very high-level introductory architecture overview provided courtesy of AWS of web application hosting in AWS cloud. It is used here to provide some context, simply illustrate some of the basic cloud hosting services available, and how you may choose to utilize them in your cloud architecture. There are literally hundreds of these services available.

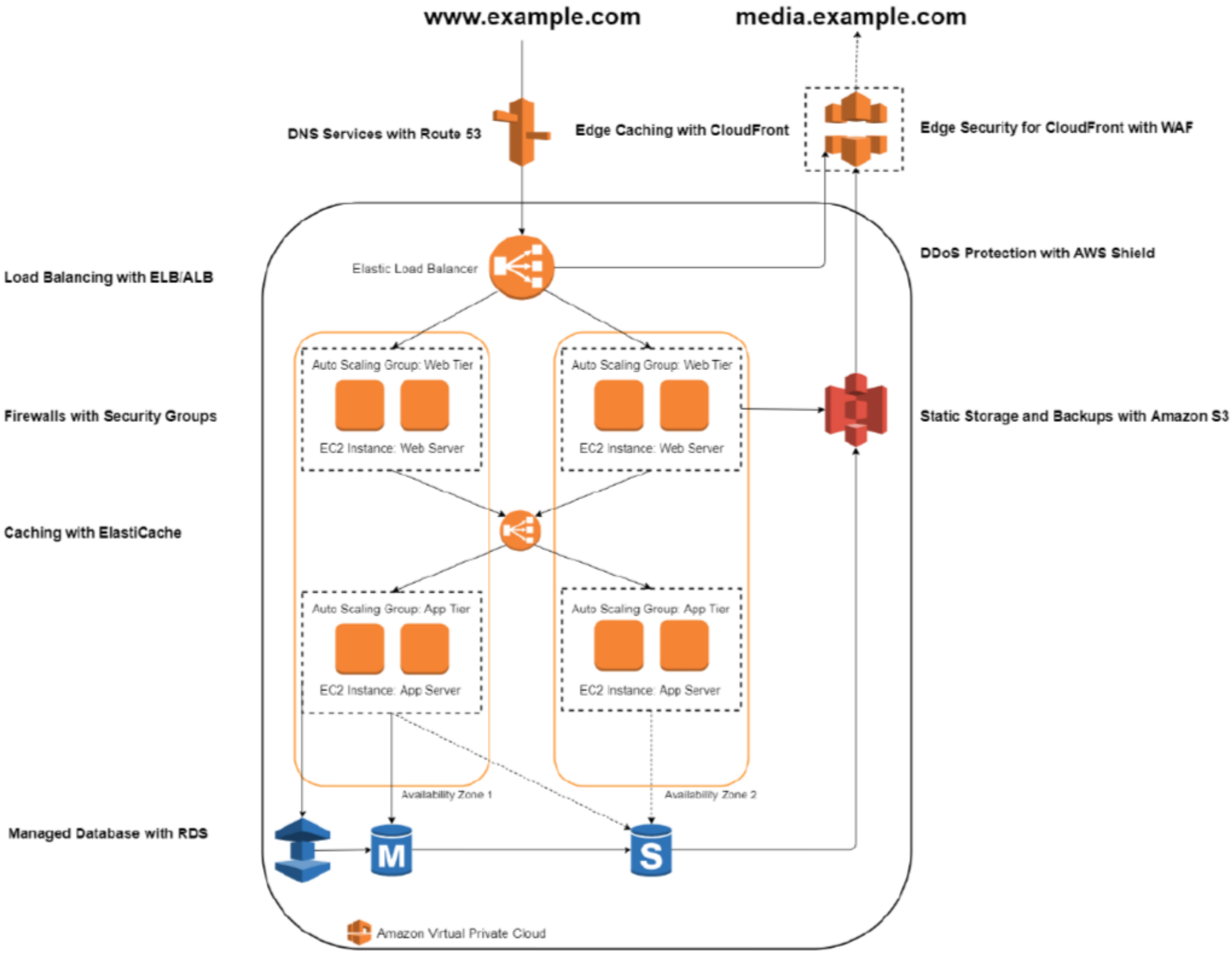

www.example.com
media.example.com
DNS Services with Route 53
Edge Caching with CloudFront
Edge Security for CloudFront with WAF
Load Balancing with ELB/ALB
Elastic Load Balancer
DDoS Protection with AWS Shield
Auto Scaling Group: Web Tier
EC2 Instance: Web Server
Auto Scaling Group: Web Tier
EC2 Instance: Web Server
Firewalls with Security Groups
Static Storage and Backups with Amazon S3
Caching with ElastiCache
Auto Scaling Group: App Tier
EC2 Instance: App Server
Auto Scaling Group: App Tier
EC2 Instance: App Server
Availability Zone 1
Availability Zone 2
Managed Database with RDS
M
S
Amazon Virtual Private Cloud

Figure Appendix 1-1 – Introductory AWS Architecture Overview

- Elastic Compute Cloud (EC2) are increments of compute resources that host, in this example, application and web server instances and allow quick capacity scaling as required.
- Application and web server EC2 instances are grouped in Auto Scaling Groups in their respective tiers.

- The Auto Scaling Groups are implemented in two distinct Availability Zones (AZ) utilizing Elastic Load Balancing (ELB) and Application Load Balancer (ALB) for redundancy, load distribution, and decoupling of services.
- Managed Database with Amazon RDS is the use of an Amazon provided DB engine that can be implemented in highly available multi-AZ architecture if the architecture calls for it.
- Caching with ElastiCache would be employed to remove load from the application and database and lower latency for frequent requests.
- Firewalls with Security Groups moves security to the instance to provide a stateful, host-level firewall for both web and application servers.
- Static Storage and Backups with Amazon S3 enables simple HTTP-based object storage for backups and static assets like images and video.
- Amazon Virtual Private Cloud (VPC) allows you to launch resources in a logically isolated and virtual network that you define, encapsulating all of the above services (the outermost grouping in Figure Appendix 1-1).
- DNS Services with Amazon Route 53 provides DNS services in this example.
- Edge Caching with Amazon CloudFront edge caches high-volume content to decrease the latency to users.
- Edge Security for Amazon CloudFront with AWS WAF filters malicious traffic,
- DDoS Protection with AWS Shield safeguards your infrastructure automatically against the most common network and transport layer DDoS attacks.

AWS Landing Zone

The AWS Landing Zone solution allows set-up of a secure multi-account environment for running secure and scalable workloads while implementing an initial baseline through the creation of core accounts and resources. It also provides a baseline environment to get started with a multi-account architecture, identity and access management, governance, data security, network design, and logging. It facilitates making design choices that would otherwise involve the configuration of multiple accounts and services, and require a deep understanding of AWS services.

A typical environment is shown in Figure Appendix 1-2 – AWS Landing Zone & Accounts Environment.

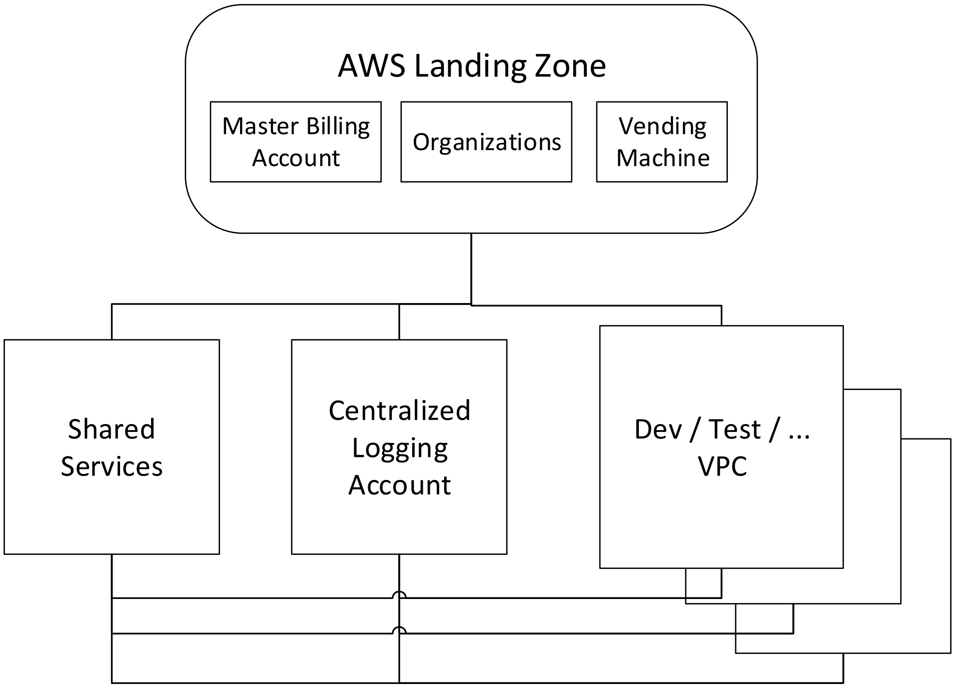


Figure Appendix 1-2 – AWS Landing Zone & Accounts Environment

Appendix 2 – OneID Azure Cost Factors Case Study

Note: the CSP in the following is for example purposes only; it is intended to be vendor-agnostic.

The guiding principles throughout this guide were put to practical use in the following exercise performed to estimate Azure Government cloud infrastructure monthly costs for OneID cloud transformation. Note that this was a 'point-in-time' exercise utilizing requirements and information available. That's especially important to illustrate the value of requirements and information discovery to evolving results of greater confidence in cost estimates.

Rough Order of Magnitude Calculation

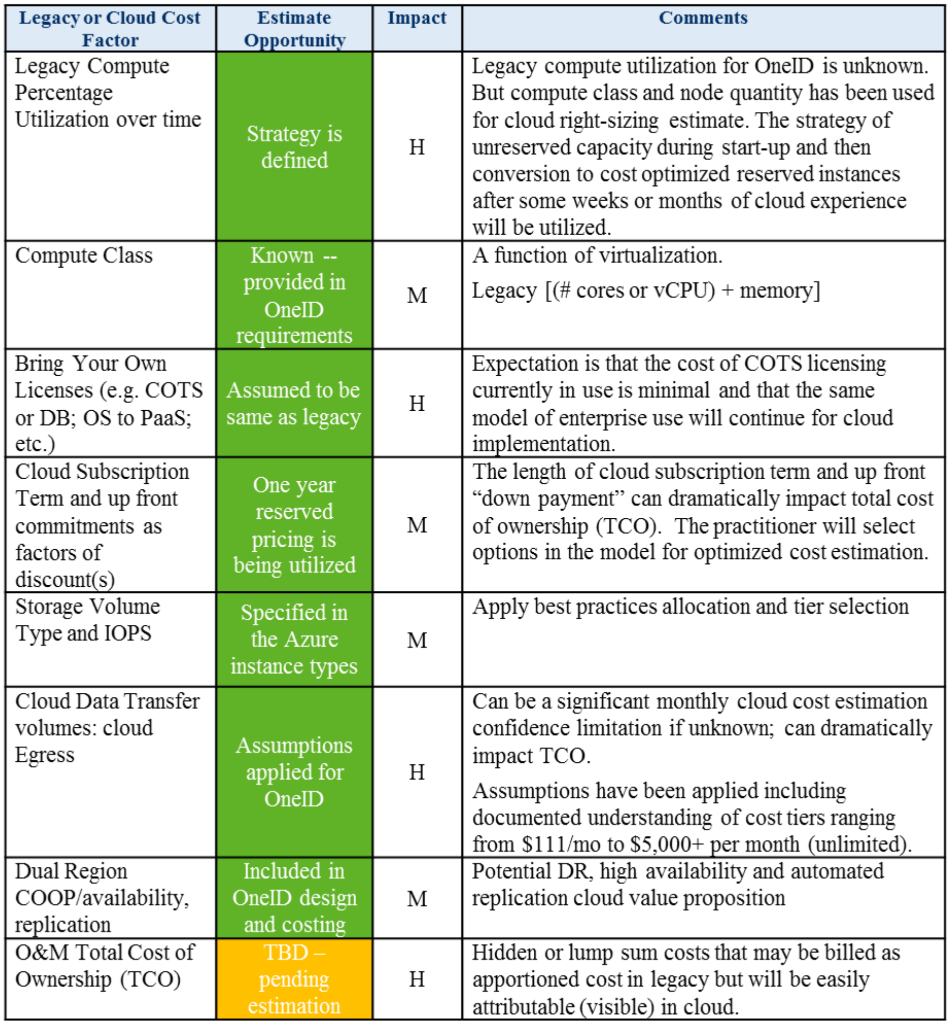
Assumptions:

- OneID data sensitivity requirement drove the CSP vendor choice of Microsoft Azure Government. Data sensitivity is FISMA Moderate; this requirement can be met by several CSP's Commercial Cloud environments. However, the additional requirement is that there be no Foreign National exposure. At the time of this writing, that could only be assured in the MS Azure Government environment.
- Financial objectives are consistent with a 1 year commitment to reserved instance capacities.
- Cloud compute classes were selected based Microsoft guidance of anticipated cloud performance when compared with legacy (current) environment configurations.
- The environments and naming that match the OneID requirements are: Dev, Test, Pre-Prod and Production; these are used for all needed functions such as QA and Performance testing.
- Infrastructure costs are estimated based on the cloud architecture, solution design and network design, utilizing the vendor provided cost estimation tool.

The following applies the analysis and estimation of cloud costs for existing transformational workloads approach laid out in *Section 10 – Business Case | Cost Factors.* Please refer to that section for explanation, if not already reviewed. *Table 10-1 – Legacy & Cloud Cost Factors* Estimate Opportunity column was filled out and appears below for this analysis as *Table Appendix 2-1.*

Cost Factors were defined to a 'green' level – reflects high confidence in Estimate Opportunity as inputs to cloud vendor estimation calculator.

O&M Total Cost of Ownership estimate is pending (orange). Confidence in this factor is important to the ROM estimate since it is of potentially high impact.

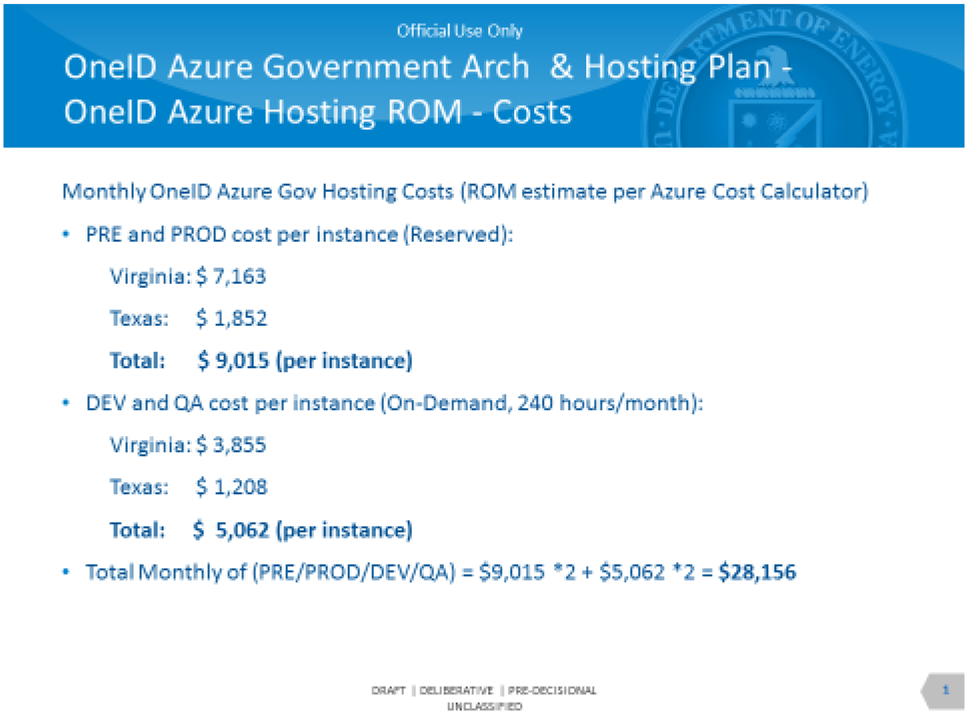


Legacy or Cloud Cost Factor	Estimate Opportunity	Impact	Comments
Legacy Compute Percentage Utilization over time	Strategy is defined	H	Legacy compute utilization for OneID is unknown. But compute class and node quantity has been used for cloud right-sizing estimate. The strategy of unreserved capacity during start-up and then conversion to cost optimized reserved instances after some weeks or months of cloud experience will be utilized.
Compute Class	Known -- provided in OneID requirements	M	A function of virtualization. Legacy [(# cores or vCPU) + memory]
Bring Your Own Licenses (e.g. COTS or DB; OS to PaaS; etc.)	Assumed to be same as legacy	H	Expectation is that the cost of COTS licensing currently in use is minimal and that the same model of enterprise use will continue for cloud implementation.
Cloud Subscription Term and up front commitments as factors of discount(s)	One year reserved pricing is being utilized	M	The length of cloud subscription term and up front "down payment" can dramatically impact total cost of ownership (TCO). The practitioner will select options in the model for optimized cost estimation.
Storage Volume Type and IOPS	Specified in the Azure instance types	M	Apply best practices allocation and tier selection
Cloud Data Transfer volumes: cloud Egress	Assumptions applied for OneID	H	Can be a significant monthly cloud cost estimation confidence limitation if unknown; can dramatically impact TCO. Assumptions have been applied including documented understanding of cost tiers ranging from $111/mo to $5,000+ per month (unlimited).
Dual Region COOP/availability, replication	Included in OneID design and costing	M	Potential DR, high availability and automated replication cloud value proposition
O&M Total Cost of Ownership (TCO)	TBD – pending estimation	H	Hidden or lump sum costs that may be billed as apportioned cost in legacy but will be easily attributable (visible) in cloud.

Table Appendix 2-1

The red/yellow/green heat map application to the Estimate Opportunity element is simply to convey a sense of the degree of confidence that is likely in the estimate. Combined with the high, medium or low impact expectation, the practitioner will gain insight into how to use cost model data for planning purposes. As a heat map, the colors of Estimate Opportunity cells were modified from the reference model table to reflect the degree to which the Estimate Opportunity is known. Accordingly, the combination of the color and the factor's Impact contribute subjectively to the OneID cloud transformation cost estimate confidence.

The rough order of magnitude cost for the AWS cloud infrastructure (at the time of this writing) and per the current design is shown in Figure Appendix 2-1.



Official Use Only

OneID Azure Government Arch & Hosting Plan -
OneID Azure Hosting ROM - Costs

Monthly OneID Azure Gov Hosting Costs (ROM estimate per Azure Cost Calculator)

- PRE and PROD cost per instance (Reserved):

Virginia:	$ 7,163
Texas:	$ 1,852
Total:	**$ 9,015 (per instance)**

- DEV and QA cost per instance (On-Demand, 240 hours/month):

Virginia:	$ 3,855
Texas:	$ 1,208
Total:	**$ 5,062 (per instance)**

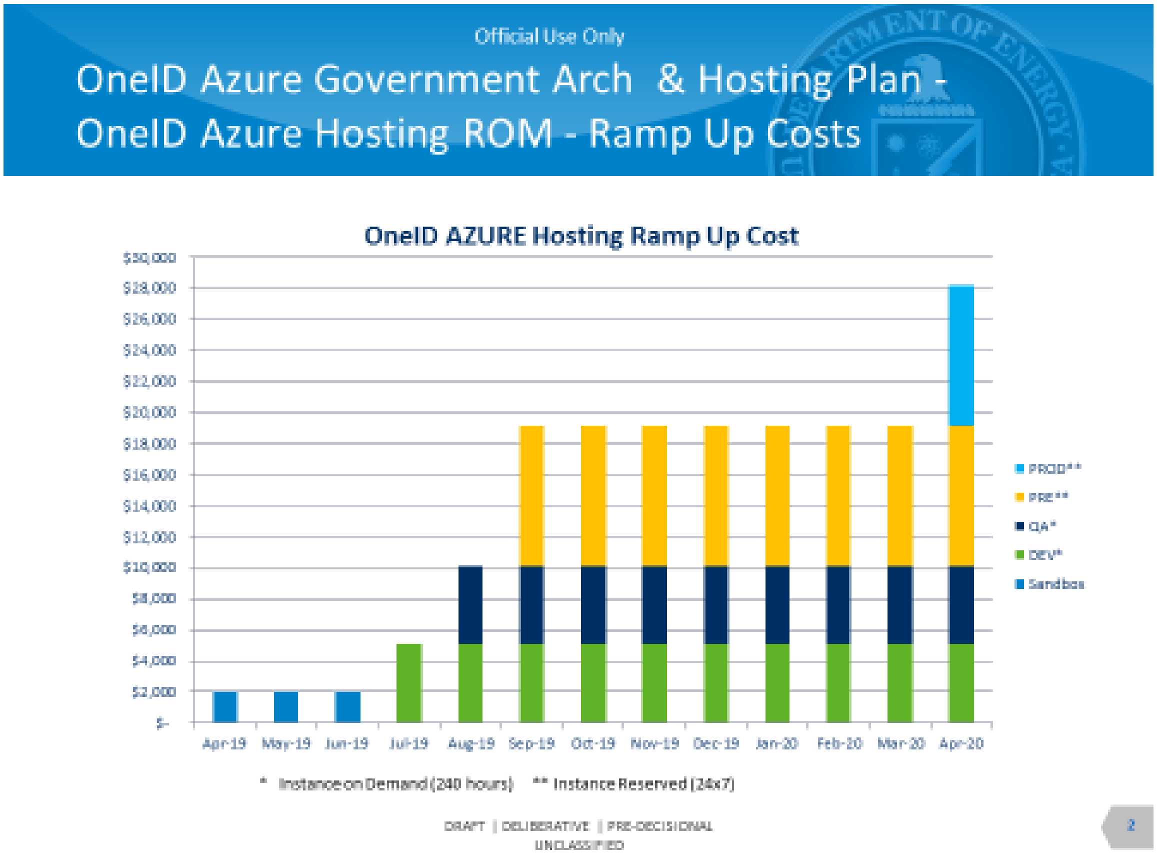
- Total Monthly of (PRE/PROD/DEV/QA) = $9,015 *2 + $5,062 *2 = **$28,156**

DRAFT | DELIBERATIVE | PRE-DECISIONAL
UNCLASSIFIED

1

Figure Appendix 2-1

The cost ramp-up in year one as it relates to the environments build-out is as estimated in Figure Appendix 2-2.



Official Use Only

OneID Azure Government Arch & Hosting Plan -
OneID Azure Hosting ROM - Ramp Up Costs

* Instance on Demand (240 hours) ** Instance Reserved (24x7)

DRAFT | DELIBERATIVE | PRE-DECISIONAL
UNCLASSIFIED

2

Figure Appendix 2-2

OneID will take advantage of some enhanced availability cloud features. Dual Region COOP/availability, replication factors are inherently value added propositions in cloud, albeit with some incremental cost. Every application cloud transformation assessment should include analysis of the opportunity to gain DR and COOP capabilities in cloud which may have been cost prohibitive in the legacy situation. Due to the flexible nature of cloud and automation, incremental costs of DR, high availability, and data replication are typically reasonable, especially compared with legacy situations.

Appendix 3 – AWS Adoption Use Case

Note: the CSP in the following is for example purposes only; it is intended to be vendor-agnostic.

There are scenarios in which it's advisable for Customers and DOE Sites (e.g. Labs) to consolidate cloud environments. These scenarios are described in the following.

Figure Appendix 3-1 depicts Scenario 1 where an example existing AWS Managed Landing Zone is leveraged with the Customer or Site becoming a tenant (left portion of the figure), and Scenario 2 where the Customer or Site applications and workloads have the opportunity to fully leverage this ecosystem by becoming a Landing Zone Client (right portion of figure).

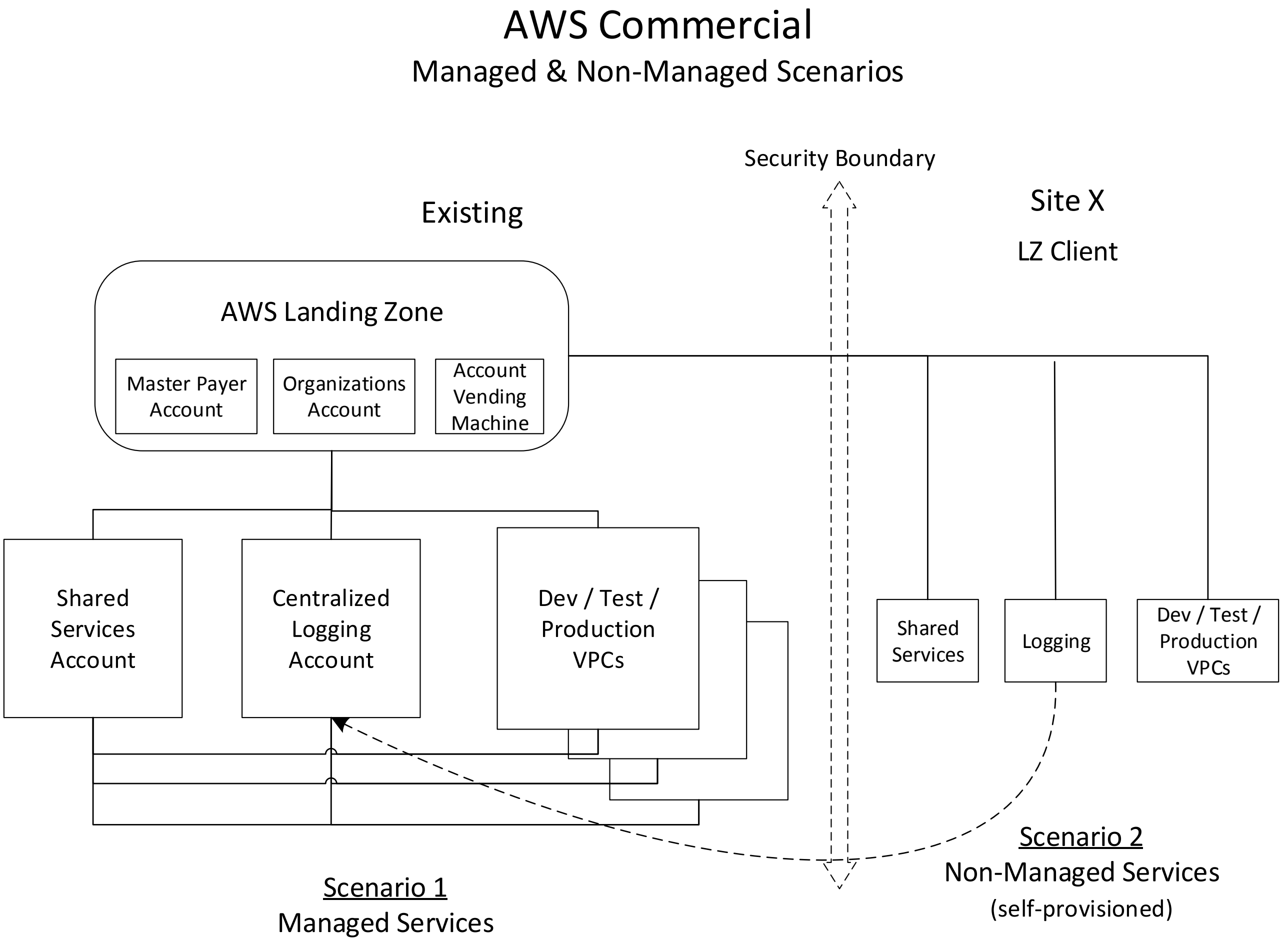


Figure Appendix 3-1 – AWS Commercial Managed & Non-Managed Scenarios

Scenario 1 is operated as managed services including all AWS services necessary to fully meet the requirements of applications and workloads migrated from the on-premises situation. It consists of the AWS Landing Zone comprised of Master Billing Account, Organizations and Vending Machine. The Landing Zone is infinitely scalable in the AWS commercial regions. Within the example AWS Security Boundary, N-number of applications and workloads make use of shared services and centralized logging and account services. Completely independent Sandbox, Development, Test and Production environments are built out in virtual private clouds.

Scenario 2 offers Customer or Site applications and workloads the opportunity to fully leverage this ecosystem by becoming a Landing Zone Client. In this scenario, self-provisioned 'non-' or 'self-managed services consisting of the Customer or Site provided shared services, logging, their own CMP tools, and completely independent Sandbox, Development, Test and Production environments with their own security boundary. Customer or Site logging data flows to the existing Centralized Logging Account for charge-back purposes.

Figure Appendix 3-2 depicts Scenario 3 in which sites may choose to stand up their own independent AWS Commercial, self-hosted cloud environment.

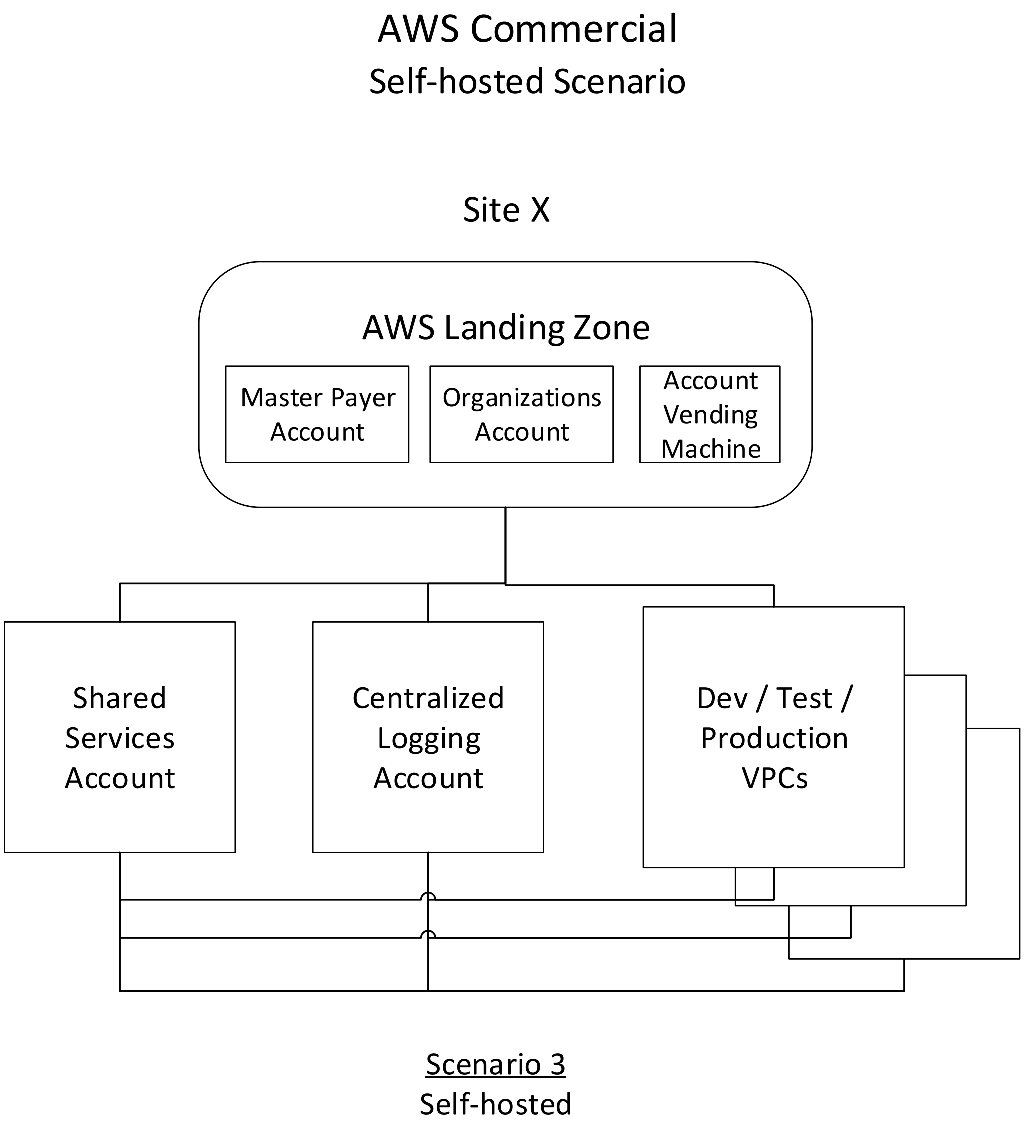


Figure Appendix 3-2 – AWS Commercial Self-hosted Scenario

While this is a viable AWS Commercial requirements alternative, the OCIO Enterprise Architecture recommendation is to first carefully consider the LOE, timeline, cost and other factors presented in this DOE *Cloud Smart Reference Guide* before embarking on such an initiative. The potential to leverage an existing Department cloud environment in a shared Landing Zone situation such as in scenarios 1, 2 and 4 should be foremost in the decision.

Figure Appendix 3-3 depicts Scenario 4 where FedRAMP AWS GovCloud is required.

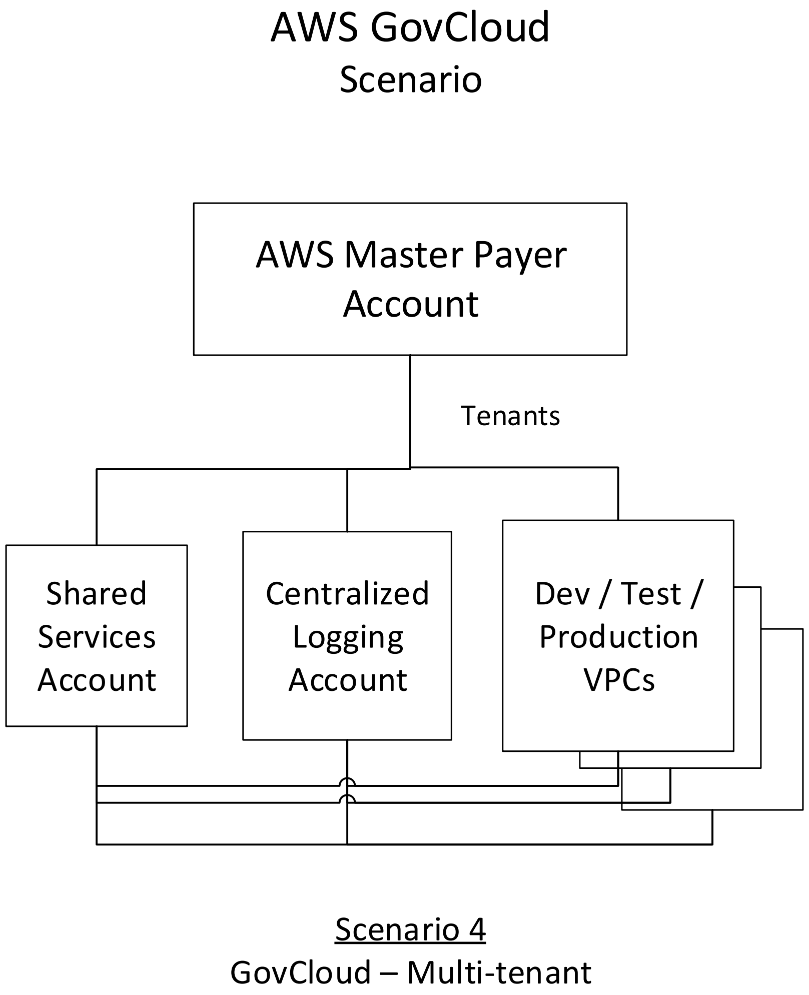


Figure Appendix 3-3 – AWS GovCloud Scenario

FedRAMP is available for AWS US-East-1 GovCloud Region in order to accommodate DOE workloads that require GovCloud. The current recommendation is for Sites to pursue operation as a tenant in a multi-tenant situation.

[END OF DOCUMENT]