Commonwealth of Virginia

Enterprise Technical Architecture (ETA)

Platform Domain Topic Report
Cloud-based Hosting Services

Version 1.0, February 04, 2019

Prepared by:
Virginia Information Technologies Agency (VITA)

Revision History

Cloud-based Hosting Services Topic Report: Version History		
Revision	**Date**	**Description**
1.0	02/04/2019	Initial
1.1	01/26/2022	Update

Review Process

This report was posted on VITA's Online Review and Comment Application (ORCA) for 30 days. All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were carefully evaluated and the individual commenters were notified of the action taken.

Definition of Key Terms

All of the Cloud-based Hosting Services Topic ETA standards and requirements considered to be critical components for implementing the Commonwealth's ETA are included in this report.

The report presents three forms of technical architecture guidance for agencies to consider when planning or when making changes or additions to their information technology:

- **Requirements** – mandatory enterprise technical architecture directions. All requirements are included within the ETA Standard.

- Technology Component Standard Tables - indicate what technologies or products that agencies may acquire at a particular point in time. These are mandatory when acquiring new or replacing existing technology or products. All technology component standard tables are included within the ETA Standard.

- *Recommended Practices* - provided as guidance to agencies in improving cost efficiencies, business value, operations quality, reliability, availability, decision inputs, risk avoidance or other similar value factors. Recommended Practices are optional.

The following terminology and definitions are applicable to the technology component standard tables presented in this report:

Strategic:

This technology is considered a strategic component of the Commonwealth's Enterprise Technical Architecture. It is acceptable for current deployments and must be used for all future deployments.

Emerging:

This technology requires additional evaluation in government and university settings. This technology may be used for evaluative or pilot testing deployments or in a

higher education research environment. Any use, deployment or procurement of this technology beyond higher education research environments requires an approved *Enterprise Architecture Change/Exception Request Form*. The results of an evaluation or pilot test deployment should be submitted to the **VITA Enterprise Architecture Division** for consideration in the next review of the Enterprise Architecture for that technology.

Transitional/Contained:

This technology is not consistent with the Commonwealth's Enterprise Technical Architecture strategic direction. Agencies may use this technology only as a transitional strategy for moving to a strategic technology. Agencies currently using this technology should migrate to a strategic technology as soon as practical. A migration or replacement plan should be included as part of the Agency's IT Strategic Plan. New deployments or procurements of this technology require an approved *Enterprise Architecture Change/Exception Request Form*.

Obsolescent/Rejected:

This technology may be waning in use and support, and/or has been evaluated and found not to meet current Commonwealth Technical Architecture needs. Agencies shall not make any procurements or additional deployments of this technology. Agencies currently using this technology should plan for its replacement with "strategic" technology to avoid substantial risk. The migration or replacement plan should be included as part of the Agency's IT Strategic Plan.

Agency Exception Requests

Agencies that desire to deviate from the requirements or the technology component standards specified in this report must request an exception for each desired deviation and receive an approved *Enterprise Architecture Change/Exception Request Form* prior to developing, procuring, or deploying such technology or not complying with a requirement specified in this report. The instructions for completing and submitting an exception request are contained within the *Commonwealth Enterprise Architecture Policy*.

Glossary

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page on the VITA website at.
https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/comp-ITRMGlossary-v3.1.a-2018.pdf

Table of Contents

Introduction

The purpose of this topic report is to provide direction on how the commonwealth will create, govern and utilize cloud-based hosting services. In accomplishing this, wherever possible and appropriate, the commonwealth has adopted or built upon international, federal/national-wide, and/or widely adopted IT guidance.

This topic report applies to everyone providing and managing the provision of cloud-based hosting services for COV IT solutions, including those not considered part of the VITA enterprise.

Even though traditional hosting services remain important to meeting agency business needs, the creation and utilization of new and enhanced cloud-based IT hosting services can offer agencies/customers the following advantages:

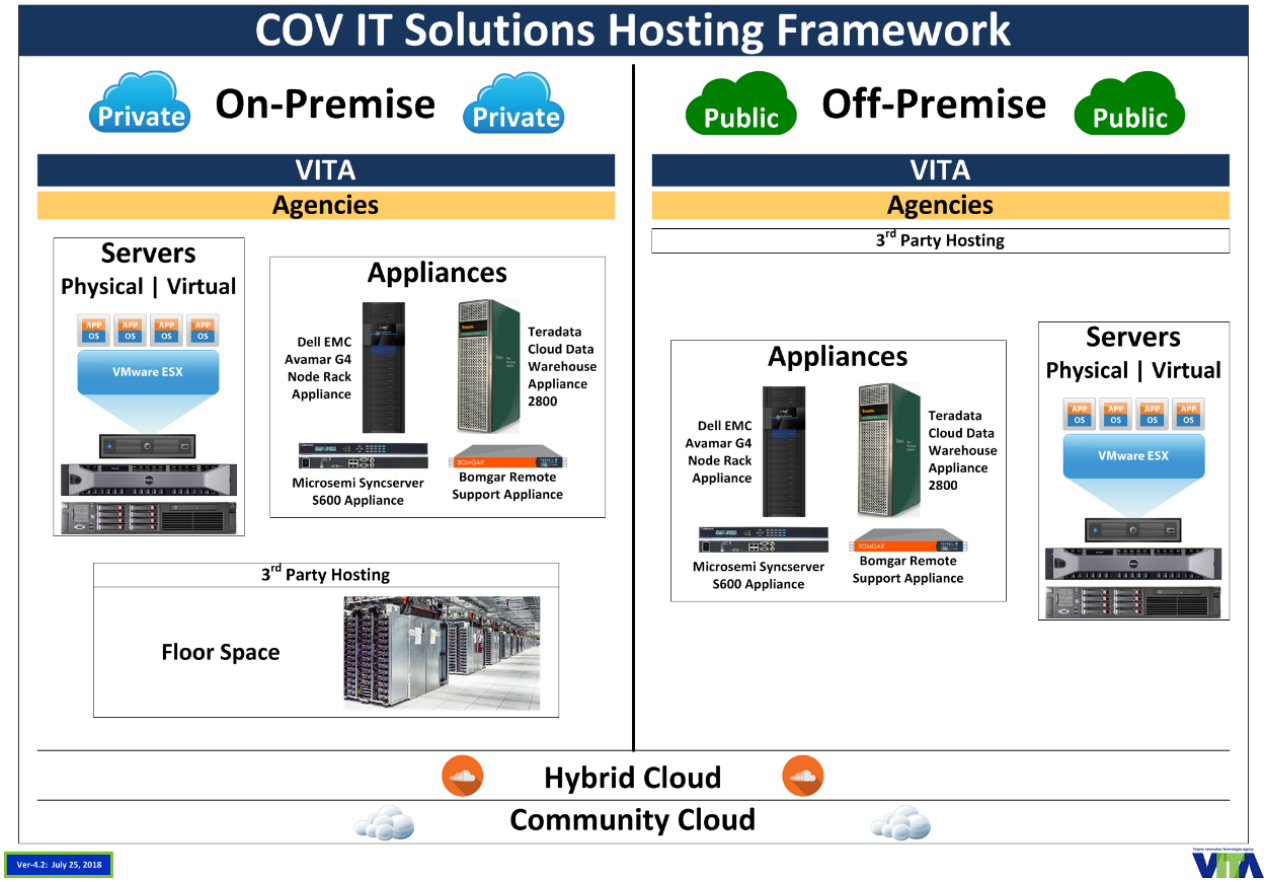
- increased flexibility
- more choices for hosting services
- multiple service level options
- faster provisioning/self-provision of services
- the ability to scale up and scale down services as needed
- the ability to be charged only for what they use or by fixed service prices
- leverage with the suppliers to obtain responsiveness

The commonwealth can also leverage these services to:

- **Reduce time to market:** implement new business solutions more quickly so revenue comes in faster
- **Better enable the solution development life cycle:** speed up business solutions through better facilitation for development and testing and overall faster paths to production
- **Respond to business change:** new requirements of existing business solutions are met more quickly
- **Enhance transparency of IT costs:** customers are more aware of what they get for their money
- **Consistently deliver to better-defined service levels:** leads to increased customer satisfaction
- **Provide better continuity of service:** minimize service interruptions
- **Ensure regulatory compliance:** meeting or exceeding mandatory requirements, which may grow more complex with online services

IT Solutions Hosting Services Framework

The commonwealth has adopted an IT service hosting framework to provide deployment models for the delivery of IT solutions. The hosting services must provide flexible options for deploying agency/customer IT solutions in order to meet different and evolving needs for security, reliability, scalability, availability, portability, mobility, performance, and service levels. The hosting framework includes on-premise and off-premise hosting options:



The COV IT service hosting framework supports both cloud-based and traditional (non-cloud) models for hosting services.

Cloud-based Hosting Services for IT Solutions Policy

Vision
The commonwealth will provide a comprehensive portfolio of cloud-based IT solution hosting services, maximize cloud readiness, enable informed hosting decision-making by agencies/customers while ensuring and maintaining the appropriate security of commonwealth data. (adopted by VITA Customer Advisory Council (CAC))

Strategy
The commonwealth will: • Deploy cloud-based IT solution hosting services integrated with traditional and other hosting services • Create COV ITRM standards to support this policy, vision, and strategy • Apply governance to all IT hosting services while ensuring vulnerabilities, risks, and impacts to business operations are weighed against the advantages of adopting cloud-based hosting services for specific agency/customer IT solutions **Agencies/customers will:** • Evaluate all existing and new IT solutions for cloud readiness as defined by COV policies and standards • Determine the future state for all existing IT solutions • Develop business cases to determine if current IT solutions that could be made cloud ready should be migrated to cloud-based services (private, community, public, and/or hybrid) • Ensure all new IT solutions will either be cloud ready, or will have documented and approved business/technical exceptions • Utilize cloud-based services for all cloud ready IT (new or existing) solutions or have a documented business rationale for not using those services

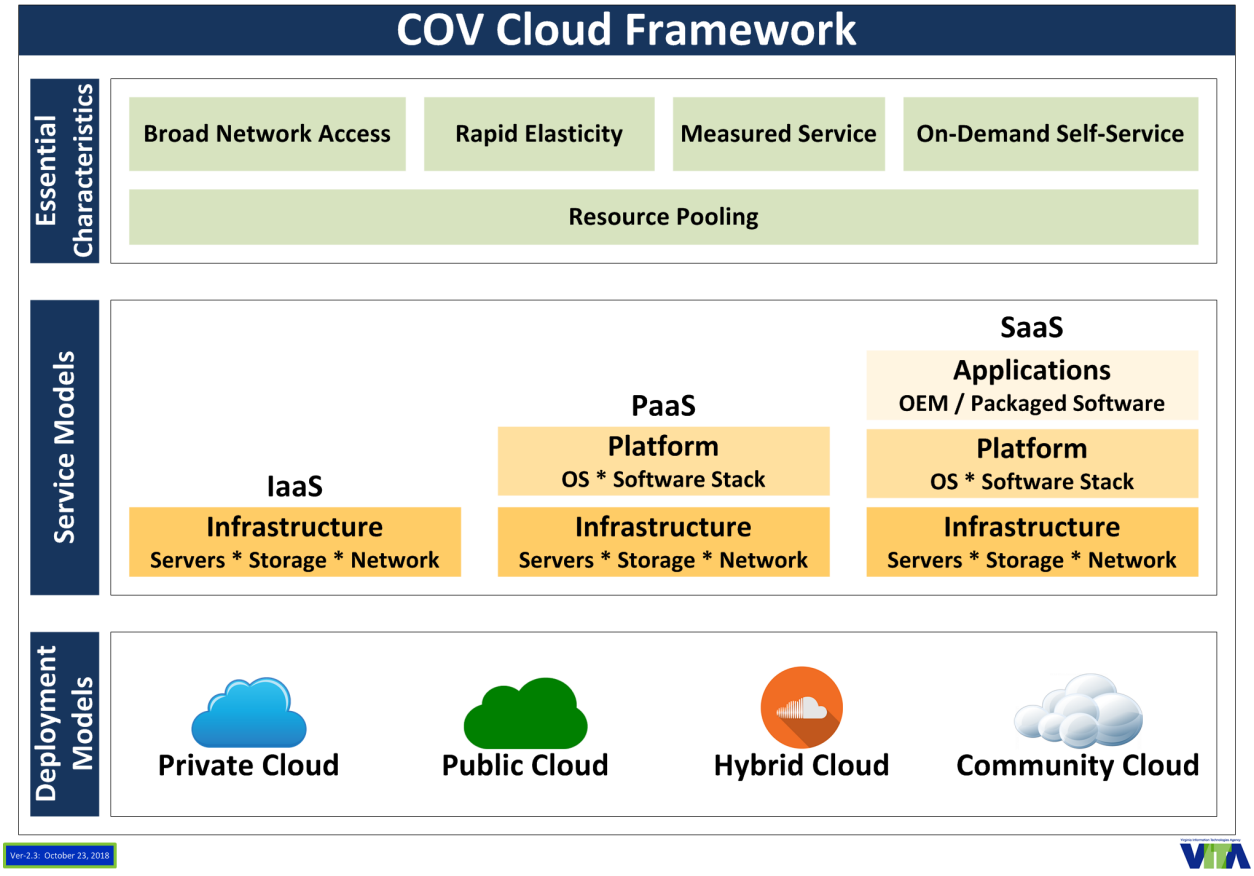
This report identifies the five following objectives to support the above vision and strategy:

Commonwealth Cloud-based Hosting Services Objectives
1. **Framework –** Publish COV definitions of cloud computing and establish a cloud-based IT solution hosting framework that adheres to those definitions 2. **Services –** Select, implement, and integrate cloud-based hosting services needed for IT solutions 3. **Suppliers –** Define COV compliant cloud-based hosting supplier service requirements 4. **Agencies/customers –** Establish and implement a methodology for how to determine which cloud-based hosting services can and should be consumed for agency IT solutions 5. **Governance –** Define and implement governance processes for cloud-based hosting services

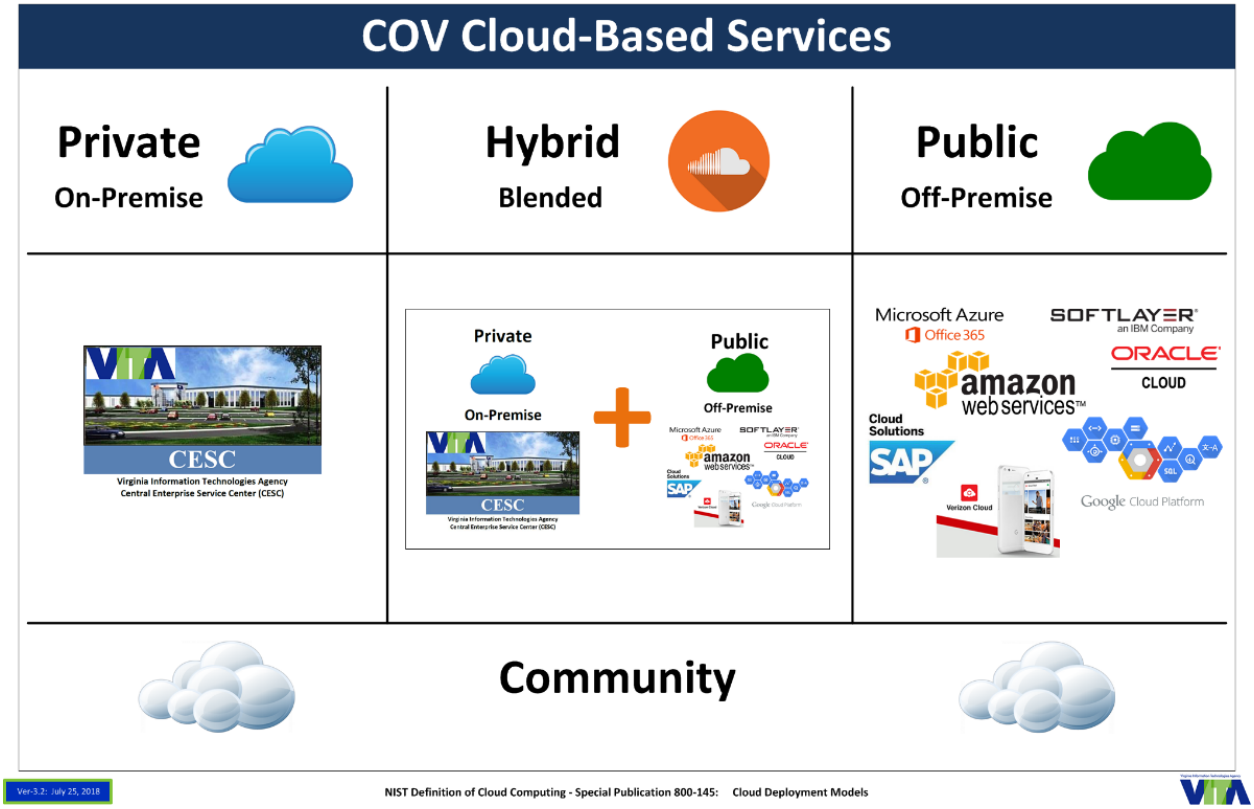
Objective 1: Framework

Publish COV definitions of cloud computing and establish a cloud-based IT solution hosting framework that adheres to those definitions

CBH-R-01: **Define the cloud-based hosting services within the framework –** COV cloud-based services shall cover all COV defined services and deployment models, will meet all five of the characteristics and will be deployed both on-premise and off-premise as follows:



Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Three Service Models

Infrastructure as a Service (IaaS) - the capability provided to the consumer is 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, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service (PaaS) - the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. 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 configuration settings for the application-hosting environment.

Software as a Service (SaaS) - the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. 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.

Four Deployment models

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). 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.

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

Public cloud - the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). *The COV hybrid cloud will consist of at least one private cloud, more than one public (utility) cloud, more than one community (gov/FedRAMP) cloud, and integration between these cloud hosting services.*

Five Essential Characteristics

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

Broad network access - capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service - cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of

service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Readiness

Cloud readiness is defined as an IT solution that is either already hosted or can be hosted on a virtual server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services.

Determining Migration Path of Commonwealth IT Solutions

There are nine possible migration paths for each agency/customer IT solution that is not already hosted by cloud-based services.

1. **Retire/Remove –** (decommission), retire the solution in a controlled manner, preserving essential data. Care should be taken to ensure that the service is decommissioned in a fashion that is in line with your current procedure of retiring an IT solution, but often times a data center renovation is a great time to remove deprecated technology from the portfolio. In today's data centers there are often times several workloads that are no longer used but have been kept running.

2. **Retain –** (contain), perform minimum upkeep to the solution to maintain security etc. for the minimum cost (no major changes or investments will be allowed). This retain methodology often times is used in a hybrid cloud deployment that uses some on-premises IT servers and services combined with cloud technologies to offer a seamless integrated user experience. Retaining old solutions typically brings with it increased costs to maintain. In addition to hardware support that tends to become more expensive as spare parts become scarce, the organizational knowledge of those technologies tends to become increasingly scarce as people within the IT organization move into new roles. While it might at times make sense to retain a technology, doing so is only advisable in select circumstances. A decision to retain needs to be revisited annually to make sure the business case is still valid.

3. **Reuse –** replace current IT solution by utilizing an existing cloud-based hosted COV enterprise or agency collaborative IT solution.

4. **Rehost –** otherwise, known as "lift-and-shift", this involves moving your existing physical and virtual servers as is into a compatible PaaS solution. Rehosting is an important approach for a large legacy migration scenario where the organization is looking to complete its migration quickly to meet a business case. Example:
    - Deploying a Java application server on a Linux x86 server instead of Solaris SPARC-based server

5. **Re-platform –** "lift-tinker-and-shift" the technology. Often times when organizations have legacy IT solutions that can't be simply migrated to PaaS cloud-based hosting platforms, it is possible to run those applications on modern cloud based PaaS servers using compatibility tools and emulators to enable the use of newer cloud technologies. In general, the core architecture of the application does not change.

6. **Refactor/Re-architect/Re-image/Remediate (PaaS) –** make application code or configuration changes to allow the IT solution to consume cloud-based hosting services. Existing programming models, languages and frameworks can be used and extended. Necessary changes vary from none to widespread code changes to invoke new APIs. Refactor is "backward-compatible" PaaS. This is typically driven by a strong business need to add features, scale, or performance that would otherwise be difficult to achieve in the solution's existing environment. Examples:
   - Linking in a new database driver, identity management system, or authentication module
   - Moving a Java EE application from IBM WebSphere to Red Hat JBoss (the same type of container, some different frameworks and configuration)

7. **Revise (PaaS) –** modify or extend the existing codebase to support legacy modernization requirements, then use rehost or refactor options to deploy to the cloud. The scale of changes encompasses major revisions to add new functionality or to re-architect the application for the cloud.

8. **Rebuild (PaaS) –** discard code for an existing IT solution and rebuild to utilize a cloud-based hosting platform. This requires re-architecting the application. Not all existing programming models, frameworks, and languages can be retained when taking this approach.

9. **Replace/Repurchase (SaaS) –** discard an existing IT solution (or set of applications), assess current and to-be business requirements, and use commercial software (SaaS or COTS) hosted on cloud-based hosting platforms to satisfy those business requirements. Typically, existing data requires migration to the new environment. Examples include moving:
   - CRM to Salesforce.com
   - An HR system to Workday
   - A CMS to Drupal

Six cloud readiness determinations

1. **Already hosted on cloud-based services –** IT solution has achieved the desired future (to-be) state for consumption of cloud-based services

2. **Cloud ready**

   Prefered – IT solution is hosted on a virtual x86 or equivalent server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services. This also includes any IT solution under ECOS evaluation.

   Acceptable – IT solution is hosted on a non Windows/Linux virtual machine (examples: AIX, Solaris) that could be hosted by either a private cloud or by a community/public cloud provider where there are no software licensing or data issues with the solution consuming those cloud-based hosting services.

3. **Not currently cloud ready and cannot be made ready –** IT solution is not currently cloud ready and it may or may not be possible for it to become cloud ready

4. **Not currently cloud ready, can be and should be made cloud ready –** the IT solution can technically be made cloud ready and there is a business case for doing so

5. **Not currently cloud ready, can be but should not be made cloud ready –** the IT solution can technically be made cloud ready and there is not a business case for doing so

6. **Does not apply –** PC deployed IT solution that included no server-based components

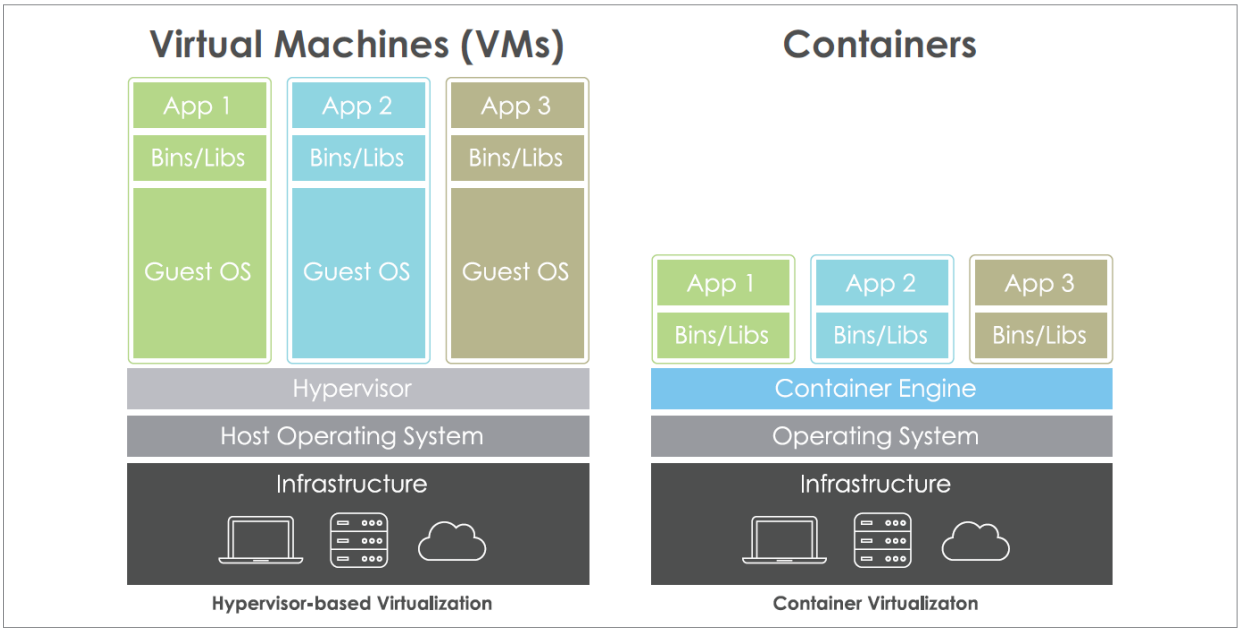
The cloud readiness determinations map to the cloud-based hosting services migration paths as follows:

Map of Cloud Readiness to IT Solution Migration Path	
Cloud Readiness Determination	**IT Solution Migration Path**
Already hosted on cloud-based services	*None*
Cloud ready	Rehost Re-platform
Not Currently Cloud Ready	
Cannot be made ready	Retire/Remove Retain
Can be and should be made cloud ready	Reuse Refactor/Re-architect/Re-image/Remediate Revise Rebuild Replace/Repurchase
Can be but should not be made cloud ready	Retain
Does not apply	*None*

Containers/Containerization

A container is a packaging format that encapsulates a set of software with its dependencies and runs in a virtual server environment with a minimal operating system (OS). Therefore, it is a form of virtualization. The difference between VM's and containers is that each VM has its own full sized OS, while containers have a minimal OS. Containerization is the encapsulation of an application in a container.

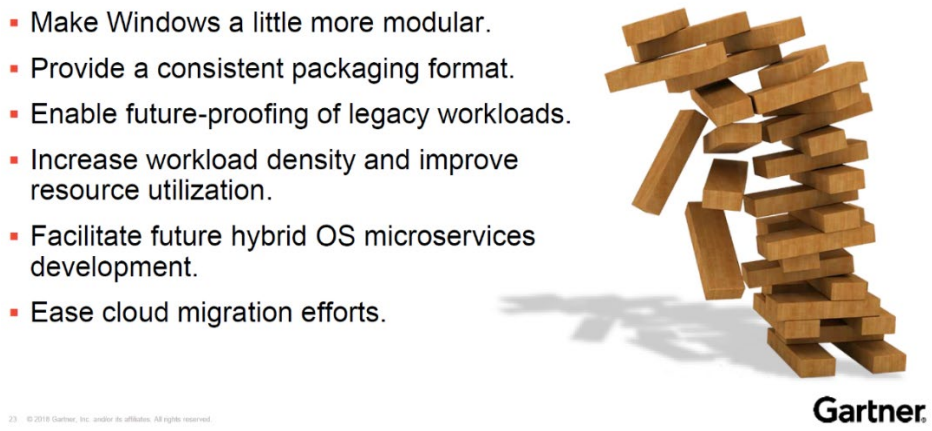
A physical server running three virtual machines would have a hypervisor and three operating systems running on top of it. A container would be a server running three containerized applications on a single operating system sharing the operating system kernel using a software tool to cluster the CPU's into a single virtual host.



Containers solve the problem of how to get *"software"* to run reliably when moved from one computing environment to another.

Pros

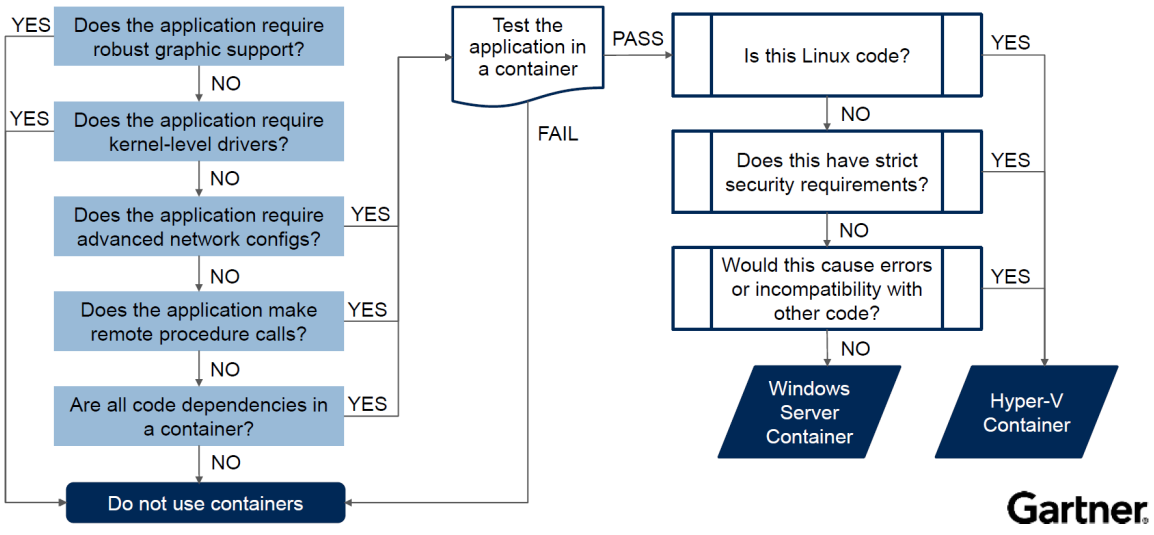
- Containers are lightweight and use far fewer resources than virtual machines. Therefore, a single server can host far more containers than virtual machines and it could be quicker to spin up containers than a virtual machine.
- Containerization allows for modularity. A developer that would normally run a complex application inside a single container could split the application into modules. Thus, the application becomes easier to manage, because each module becomes relatively simple to manage. Application changes would apply directly to the modules instead of rebuilding the application.
- Application Development of (net-new) applications is the primary adopted use for containerization.
- Containerization supports portability. Applications can be migrated between platforms with relative ease.



Cons

- Not all applications fit the container model.
- Security is a major concern, because containers share a common OS kernel.
- Lose visibility and control over what's running in your infrastructure.
- Management tools to orchestrate large numbers of containers are not as comprehensive currently as a virtual machine environment.
- The networking complexity of container applications coexistence with virtual machines applications as well as public or private cloud applications can require a major effort.

Choosing an Application Delivery Method



Objective 2: Services

Select, implement, and integrate the cloud-based hosting services that are needed for COV IT solutions

CBH-R-02: **COV Cloud-based hosting service models –** the commonwealth COV cloud-based services models shall include Platform as a Service (PaaS) and Software as a Service (SaaS) service models.

CBH-RP-01: *COV Cloud-based hosting deployment models* – the commonwealth COV cloud-based hosting deployment models should consist of:

- at least one private cloud (on-premise or co-located) with ability to host local community cloud,
- more than one public cloud,
- more than one community cloud, and
- integration between those cloud-based hosting services (hybrid cloud).

CBH-R-03: **COV cloud-based hosting services –** cloud-based hosting services shall conform to the following five essential cloud characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

CBH-R-04: **Commonwealth data concerns –** cloud-based service suppliers and the CSB shall document and provide the answers to the following questions for all cloud-based services that host commonwealth data:

- Who owns the data?
- Where is the data located?
- How does the commonwealth get the data back?
- How does the commonwealth confirm the data is deleted?
- How is the data secured?
- How does the commonwealth confirm that the data is secure?

CBH-RP-02: *Paying for features that are not needed* – the Cloud Service Broker should ensure the cloud-based hosting suppliers have documented and provided how they construct services so that agencies/customers do not pay for features that they do not need.

CBH-R-05: **Proposed service cost modeling and service use cost estimation modeling –** COV cloud-based hosting services shall include the functionality to allow customers to:

- Compare costs for hosting their IT solution among the proposed deployment and service models
- Project spending on hosting services
- Monitor and track use and cost

CBH-RP-03: *Customer billing methods* **–** all cloud deployment models should have a billing method that indicates the type of billing method that is being used and the resources that will be allocated to the agency. The billing methodology should address both:

- *Fixed recurring fees:* fully dedicated resources to an agency's use that will not be scaled up or down within a given billing period.
- *Pay for what you use*: resource allocation that may change at any time during the billing period

CBH-R-06: **Cloud-based service integration model –** Cloud services will be offered through a Cloud Service Broker (CSB) integration model. All enterprise cloud services shall integrate any existing and future cloud-based hosting services into the CSB model. The CSB shall at a minimum include the following features:

- Provide an extended hybrid cloud management tool
- Provide new service onboarding
- Integrate with the VITA service catalog/app store
- Provide cost modeling
- Provide cost monitoring (expenditures vs. budgeted)
- Connect CSB applications to single sign-on services for end users
- Support end-to-end monitoring
- Provide unified billing and reporting
- Report performance and utilization information
- Integrate and enforce commonwealth's governance requirements

CBH-RP-04: *Portfolio of contracts* – the COV should have access to multiple contracts with multiple suppliers for each of the service models. These contracts should be for six years or less (not including optional extensions).

CBH-R-07: **Cloud-based hosting service contracts –** the Cloud Service Broker (CSB) shall ensure that the commonwealth and its customers have the provision to "get out" of a cloud-based hosting contract if needed/required.

CBH-RP-05: *Consider pursuing back office IT solutions SaaS contracts* – the commonwealth should consider creating contracts for back office SaaS services with multiple awards (convenience contracts) for multiple back office functions. Examples of SaaS of interest include:

Software as a Service (SaaS)	
Customer Relationship Management (CRM)	
ERP	HR Finance • Accounts Payable / Receivable • General Ledger Budget Procurement
GIS	Basemaps – Bing, Google, ESRI Cartography and visualization Large data storage and services (aerial photography, imagery) Geospatial data sharing
Human Resources	Payroll Time, Attendance and Scheduling Recruitment and Hiring

CBH-R-08: **Cloud-based hosting services support of containers –** the COV hybrid cloud-based hosting services shall include support of containers.

Objective 3: Suppliers

Define COV compliant cloud-based hosting supplier service requirements

For VITA supported agencies, the cloud-based hosting supplier services have been procured as part of the Infrastructure Sourcing efforts. These contracts can be found at the VITA Supply Chain Management (SCM) Statewide Contract Search webpage: https://vita.cobblestonesystems.com/public/.

CBH-R-09: **Compliance to COV cloud framework characteristics** – suppliers shall document how the deployment models for their services comply with COV cloud framework characteristics.

CBH-RP-06: *On-Demand self-service provisioning* – self-service capabilities for compute and storage resources should at a minimum include:

- Deploying new servers with either custom or standard/established configurations (i.e., configurations for standalone or as part of server farm)
- Deploying server images (i.e., pre-defined OS, system management, security, databases, middleware and applications) in accordance with VITA's requirements and policies
- Provisioning storage space on demand
- Allowing for alerts when provisioning and deprovisioning systems

CBH-R-10: **Customer access to support –** suppliers shall provide access to technical support for all customers (localities and executive branch agencies).

CBH-R-11: **Pricing transparency –** suppliers pricing (including estimation models) shall be transparent, accessible and integrated with the Commonwealth CSB.

CBH-R-12: **Remove barriers for consuming on-premise cloud-based hosting services –** suppliers of on-premise private cloud-based hosting services shall remove technical and financial barriers to the use of those services. This includes supporting enough cores, memory, storage, bandwidth, connectivity, throughput, and any other capability needed to support the vast majority of agency applications including their associated databases.

CBH-R-13: **Deployment technology stack with PaaS –** cloud-based hosting service suppliers shall follow an approach of providing services that include as much of the deployment technology stack required by IT solutions into PaaS as appropriate. This means the components of the deployment technology stack (database, application server, monitoring tool, etc.) should be included in PaaS services.

CBH-RP-07: *Additional CSB responsibilities* – suppliers who provide Cloud Service Broker (CSB) services are responsible for ensuring that the cloud-based services they manage:

- Document procedures and schedules for any planned downtime
- Include service(s) that can apply legal retention periods and disposition by customer's policy and/or legal requirements
- Include service(s) that include multiple data centers, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost

Objective 4: Customers

Establish and implement a methodology for how to determine which cloud-based hosting services can and should be consumed for agency IT solutions

The procurement and deployment decisions on IT solutions impact both the possible service and deployment models available and those options drive cost. For this reason, additional effort must be spent by the agencies to drive these decisions. Enabling the ability to consume additional hosting choices means the information driving service and deployment model decisions must be captured as early in the procurement process as possible.

CBH-R-14: **Application succession plan –** all IT solutions hosted off-premise shall have a plan for what could be done if circumstances arise that require the solution to be moved or migrated (what happens if the hosting entity fails, has a breach, etc.).

- This plan must be reviewed and updated as part of customer governance whenever significant changes occur to the solution, deployment, or data
- Examples of plan options to consider:
  - Can the SaaS solution migrate to another host? Optimally, there would be multiple SaaS vendors on contract and other agencies also using that same SaaS solution (this minimized risk which should be evaluated as part of the governance process)
  - Can the customer migrate to another SaaS solution (data needs to able to be exported and then imported)?
  - As a last resort, can the solution be brought back in house? Are the technologies needed strategic? (supported by VITA and partners)

CBH-RP-08: *Service model first, then deployment model* – agencies/customers should evaluate and select the service model (SaaS, PaaS) first based on their business, and information needs. Then customers should establish the appropriate VITA supplied cloud-based hosting deployment model based on the solution and technology requirements.

CBH-RP-09: *Business processes* – to consume cloud-based hosting services, both the IT solutions and the business should be ready for the cloud. To do this, all future supporting business processes should be designed to support being hosted on cloud-based services. The supporting business processes of current IT solutions need to be assessed to determine what the impact of migrating to cloud-based hosting services would have on the business.

CBH-R-15: **Assess IT solutions for cloud readiness –** all IT solutions shall be assessed for cloud readiness.

CBH-R-16: **Assess new IT solutions for cloud readiness –** all new IT solutions shall be assessed for cloud readiness as part of the procurement process.

CBH-R-17: **New IT solution hosting –** all new cloud ready IT solutions shall be hosted by cloud-based services (private, community, and/or public).

CBH-R-18: **IT Strategic Plan –** agencies/customers shall include in their IT Strategic Plans efforts to migrate to cloud-based services and other determined future states.

CBH-R-19: **SaaS vs. PaaS –** agencies/customers shall follow a tactical approach of utilizing SaaS over PaaS for back office functions and as appropriate for core business functions.

Cloud readiness

CBH-R-20: **Pursue cloud readiness –** agencies shall ensure that all new IT solutions are cloud ready and agencies shall also have a plan in place to maximize the potential of their current solutions to be cloud ready. New IT solutions are defined as solutions that are not implemented or do not have an approved strategic plan entry as of 10/1/2018.

CBH-R-21: **Cloud readiness requirements –** VITA shall create a tool that will use the defined cloud readiness attributes to establish the cloud readiness of current or proposed agency/customer IT solutions

CBH-R-22: **Support for becoming cloud ready –** VITA shall ensure that there are adequate supplier choices and resources available to assist agencies/customers in assessing cloud readiness or for migrating existing IT solutions to cloud-based hosting services. Suppliers for these resources will include:

- CAI contract,
- CSB,
- Infrastructure server services suppliers, and
- Cloud-based hosting suppliers.

CBH-R-23: **Cloud readiness assessment –** agencies shall complete the VITA cloud readiness assessment instruments, and VITA with the agencies will identify which of the following six cloud readiness determinations best fit each IT solution:

1. **Already hosted on cloud-based services –** IT solution has achieved the desired future (to-be) state for consumption of cloud-based services
2. **Cloud ready**

   Prefered – IT solution is hosted on a virtual x86 or equivalent server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services. This also includes any IT solution under ECOS evaluation.

   Acceptable – IT solution is hosted on a non Windows/Linux virtual machine (examples: AIX, Solaris) that could be hosted by either a private cloud or by a community/public cloud provider where there are no software licensing or data issues with the solution consuming those cloud-based hosting services.
3. **Not currently cloud ready and cannot be made ready –** IT solution is not currently cloud ready and it may or may not be possible for it to become cloud ready

4. **Not currently cloud ready, can be and should be made cloud ready –** the IT solution can technically be made cloud ready and there is a business case for doing so
5. **Not currently cloud ready, can be but should not be made cloud ready –** the IT solution can technically be made cloud ready and there is not a business case for doing so
6. **Does not apply –** PC deployed IT solution that included no server-based components

CBH-R-24: **Agency business cases for cloud migration –** agencies shall develop business cases that will be used to determine if current IT solutions that can be made cloud ready should be migrated to cloud-based services.

CBH-R-25: **Software Licensing Requirements –** agencies shall know all of the software licensing requirements for the two technology stacks needed for each of the IT solutions under consideration. For each technology stack component, agencies should know:

- Name of software component and vendor
- Type of licenses needed (site, instance, CPU, core, named user, concurrent, etc.)
- If the license supports virtual servers
- If the license supports cloud deployment
- It is suggested that the agencies also know: the number of licenses; who owns/provides the licenses; pricing options; and renewal schedule

CBH-RP-10: *Four perspectives* – in order to complete the cloud-based services migration path determination, agencies should look at their non-cloud ready IT solutions from four perspectives:

1. The *business*
2. The information the business needs (*data*)
3. The possible IT *solutions*
4. The *technologies* that support those solutions.

Know the business: agencies should "know the business" for each IT solution that needs cloud-based service migration path determination.

- Are the business processes documented?
- Can the business change the process vs. change the code (utilizing the cloud requires the business to change, not the cloud vendors)?
- Can SaaS configuration address the business needs for customization?
  - Supplier supported vs. agency supported models for change/support
- What are the high-level business requirements for?
  - Availability – what level of service (bronze, silver etc. meets their needs)
  - High Availability (HA), fail over, Disaster Recovery (DR)
  - What environments are needed? (training, dev & test
  - Do you need or could you use the ability to scale up or down capacity
  - What are the required hours of operation, maintenance windows?

Know the data: agencies should "know the data" for each IT solution that needs cloud-based service migration path determination.

- What is the data?
  - Conceptual model

  - Logical model
  - Physical model
  - Data Dictionary
  - Classification
- Who is data owner?
- Where is data located?
- What are the sensitivity and risks associated with the production, test, and development data?
- What are the data exchanges?
  - Are there Interconnection Security Agreements (ISA)? (SEC501)
- What are the additional controls on the data needed due to state or federal law?
- What are the backup requirements?

Know the solution: agencies should "know the solution" for each IT solution that needs cloud-based service migration path determination. Prior to cloud-based hosting services, the commonwealth approach to the replacement of IT solutions was:

1. Consider the reuse of existing applications and system components
2. If no reuse candidates exists, consider commercial off-the-shelf (COTS) solutions
3. Only solutions that provided automation of agency core business functions that had unique processes, yielded competitive advantages, or had demonstrable cost savings and/or enhanced value would be candidates for in-house IT solution development by the commonwealth

Agencies tactical approach should now be to prefer SaaS over PaaS (all back office functions and as appropriate for core business functions), and COTS vs. Custom coded. This chart shows how the IT solution acquisition approach has changed.

	Current	Future
First Choice	Reuse	SaaS
Second Choice	COTS	PaaS
Third Choice	Custom	IaaS

Know the technology: agencies should "know the technology" for each IT solution that needs cloud-based service migration path determination. Agencies should identify the technology stacks for IT solutions under consideration. Each IT solution requires:

- Deployment stack – what is needed to deploy (or run) an IT solution on a server. This includes: OS and version for every solution tier (database, application (business logic) server; presentation layer, content management, portal, etc.) and every tool (with version) needed on the servers to deploy (DB, app server, .NET etc.)
- Operations/Development stack – what is needed to develop, test, and manage the IT solution

Objective 5: Governance

Define and implement the governance processes needed for cloud-based hosting services

The commonwealth's intent is to ensure that agencies/customers do not compromise their business by trading the confidentiality, integrity, and availability of critical data and information in pursuit of the benefits cloud-based hosting services may offer. The potential IT solution vulnerabilities and impacts to business operations must be carefully and continuously assessed, then weighed against the advantages of adopting cloud-based hosting services for agency/customer IT solutions.

CBH-R-26: **Compliance to COV ITRM Policies and Standards –** supplier's cloud-based services shall comply to COV ITRM policies and standards.

CBH-R-27: **All new cloud ready IT solutions –** shall either be hosted by hybrid cloud-based services (private, community, and/or public) or will have a documented business rationale for not using those services.

CBH-R-28: **VITA Supply Chain Management (SCM) –** shall be engaged and involved in any procurement of any cloud-based hosting services.

CBH-R-29: **Virtual vs. physical servers –** New traditional hosted solutions shall be hosted on virtual servers. Use of physical servers will require an approved EA exception.

CBH-R-30: **Service and deployment model review –** processes shall be created and implemented to enable IT solution owners to select an appropriate Service Model (PaaS, or SaaS) and Deployment Service Model.

CBH-R-31: **Governance processes for Software as a Service (SaaS) –** all requests for consumption of SaaS cloud-based hosting service must be submitted for review and approval via the ECOS process.

CBH-R-32: **Governance for Platform as a Service (PaaS) –** agencies shall only consume VITA provided PaaS cloud-based hosting services.

CBH-R-33: **Architectural review –** all changes to solutions, hosting services, and choices of deployment models shall go through a formal review process. This process should have a customer internal component and if needed due to technical complexity, an integration with an external review performed by the MSI/CSB. The reviews must take a multidisciplinary approach. It is suggested that customer's internal review team include roles when appropriate of: Business Owner, Technical Owner, Security Owner, and Data Owner.

CBH-R-34: **Governance for Platform as a Service (PaaS) –** agencies shall review all of their IT solutions annually to ensure that the solution is consuming the appropriate hosting service.

Appendix A: Definitions

The NIST framework is composed of three service models, four deployment models, and five essential characteristics. The following definitions are from: *The NIST Definition of Cloud Computing; 800-145; September 2011.*

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Three Service Models

Service Models		
IaaS	PaaS	SaaS

Infrastructure as a Service (IaaS) - the capability provided to the consumer is 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, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service (PaaS) - the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. 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 configuration settings for the application-hosting environment.

Software as a Service (SaaS) - the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. 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.

Four Deployment models

Service Models		
IaaS	PaaS	SaaS
Deployment Models		
Hybrid Cloud		
Private Cloud	Community Cloud	Public Cloud

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). 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 options include: (Microsoft Cloud Services Foundation Reference Model (CSFRM)

- ***Self-hosted Private Cloud -*** a Self-hosted Private Cloud provides the benefit of architectural and operational control, utilizes the existing investment in people and equipment, and provides a dedicated on-premises environment that is internally designed, hosted, and managed.
- ***Hosted Private Cloud -*** a Hosted Private Cloud is a dedicated environment that is internally designed, externally hosted, and externally managed. It blends the benefits of controlling the service and architectural design with the benefits of datacenter outsourcing.
- ***Private Cloud Appliance -*** a Private Cloud Appliance is a dedicated environment procured from a supplier that is designed by that supplier with provider/market driven features and architectural control, is internally hosted, and externally or internally managed. It blends the benefits of using predefined functional architecture and lower deployment risk with the benefits of internal security and control.

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

Public cloud - the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). *The COV hybrid cloud will consist of at least one private cloud, more than one public (utility) cloud, more than one community (gov/FedRAMP) cloud, and integration between these cloud hosting services.*

Five Essential Characteristics

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

Broad network access - capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

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

Additional Hosting Options

Traditional – traditional hosting services include physical and virtual servers that do not meet the five NIST characteristics defined above. These services can be provided on-premise or off-premise (eGov). Implementation of a hybrid cloud model could be extended to cover these type of services within the service and management model.

Appliances - generally a separate and discrete hardware device with integrated software (firmware), specifically designed to provide a specific computing resource. These are generally "closed and sealed" – not serviceable by the owner. The hardware and software are pre-integrated and pre-configured before delivery to customer, to provide a "turn-key" solution to a particular problem. Unlike general purpose computers, appliances are generally not designed to allow the customers to change the software (including the underlying operating system), or to flexibly reconfigure the hardware.

On-premise vs. Off-premise

On-premise – a site or portion of a site (colocation) that is fully under control of the commonwealth or its delegated representatives. It may be either at a centralized COV datacenter facility, an agency datacenter/location or co-located (caged, etc.). Full control would include servers, storage, switches, the building, cooling, power, bandwidth physical security, etc.

Off-premise – any IT application hosting option that is not provided within an on-premise or colocation solution. The hosting site and environment is not under full control of the commonwealth or its designees (ex. public cloud suppliers).

A colocation (colo) - a data center facility in which a business can rent space for servers and other computing hardware. Typically, a colo provides the building, cooling, power, bandwidth and physical security while the customer provides servers and storage.

Cloud Service Broker (CSB) - an entity (real or virtual) that manages the use, performance and delivery of cloud services, in addition to enabling the negotiations and relationships between cloud providers and cloud consumers. NIST defines CSB as an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via *three primary roles including aggregation, integration and customization brokerage*.

Cloud Service Integrator (CSI) - specializes in the integration of cloud hosted services (sometimes referred to as Integration-as-a-Service). For the extended hybrid cloud model some of the IT solutions, services and data are maintained locally, while others are served remotely via multiple cloud providers.

Container - a packaging format that encapsulates a set of software with its dependencies and runs in a virtual server environment with minimal OS. Therefore, it is a form of virtualization. The difference between VM's and containers is that each VM has its own full sized OS, while containers have a minimal OS.

Containerization - the encapsulation of an application in a container.

Cloud readiness

Cloud Readiness / Cloud ready - Cloud readiness is defined as an IT solution that is either already hosted or can be hosted on a virtual server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services.

There are nine possible migration paths for each agency/customer IT solution that is not already hosted by cloud-based services.

1. ***Retire/Remove –***(decommission), retire the solution in a controlled manner, preserving essential data. Care should be taken to ensure that the service is decommissioned in a fashion that is in line with your current procedure of retiring an IT solution, but often times a data center renovation is a great time to remove deprecated technology from the portfolio. In today's data centers there are often times several workloads that are no longer used but have been kept running.

2. ***Retain–***(contain), perform minimum upkeep to the solution to maintain security etc. for the minimum cost (no major changes or investments will be allowed). This retain methodology often times is used in a hybrid cloud deployment that uses some on-premises IT servers and services combined with cloud technologies to offer a seamless integrated user experience. Retaining old solutions typically brings with it increased costs to maintain. In addition to hardware support that tends to become more expensive as spare parts become scarce, the organizational knowledge of those technologies tends to become increasingly scarce as people within the IT organization move into new roles. While it might at times make sense to retain a technology, doing so is only advisable in select circumstances. A decision to retain needs to be revisited annually to make sure the business case is still valid.

3. ***Reuse –*** replace current IT solution by utilizing an existing cloud-based hosted COV enterprise or agency collaborative IT solution.

4. ***Rehost –*** otherwise, known as "lift-and-shift", this involves moving your existing physical and virtual servers as is into a compatible PaaS solution. Rehosting is an important approach for a large legacy migration scenario where the organization is looking to complete its migration quickly to meet a business case. Example:
    - Deploying a Java application server on a Linux x86 server instead of Solaris SPARC-based server

5. ***Re-platform–*** "lift-tinker-and-shift" the technology. Often times when organizations have legacy IT solutions that can't be simply migrated to PaaS cloud-based hosting platforms, it is possible to run those applications on modern cloud based PaaS servers using compatibility tools and emulators to enable the use of newer cloud technologies. In general, the core architecture of the application does not change.

6. ***Refactor/Re-architect/Re-image/Remediate (PaaS)* –** make application code or configuration changes to allow the IT solution to consume cloud-based hosting services. Existing programming models, languages and frameworks can be used and extended. Necessary changes vary from none to widespread code changes to invoke new APIs. Refactor is "backward-compatible" PaaS. This is typically driven by a strong business need to add features, scale, or performance that would otherwise be difficult to achieve in the solution's existing environment. Examples:
   - Linking in a new database driver, identity management system, or authentication module
   - Moving a Java EE application from IBM WebSphere to Red Hat JBoss (the same type of container, some different frameworks and configuration)

7. ***Revise (PaaS)* –** modify or extend the existing codebase to support legacy modernization requirements, then use rehost or refactor options to deploy to the cloud. The scale of changes encompasses major revisions to add new functionality or to re-architect the application for the cloud.

8. ***Rebuild (PaaS)* –** discard code for an existing IT solution and rebuild to utilize a cloud-based hosting platform. This requires re-architecting the application. Not all existing programming models, frameworks, and languages can be retained when taking this approach.

9. ***Replace/Repurchase (SaaS)* –** discard an existing IT solution (or set of applications), assess current and to-be business requirements, and use commercial software (SaaS or COTS) hosted on cloud-based hosting platforms to satisfy those business requirements. Typically, existing data requires migration to the new environment. Examples include moving:
   - CRM to Salesforce.com
   - An HR system to Workday
   - A CMS to Drupal

There are six cloud readiness determinations

1. ***Already hosted on cloud-based services –*** IT solution has achieved the desired future (to-be) state for consumption of cloud-based services

2. ***Cloud ready –*** IT solution is hosted on a virtual x86 or equivalent server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services. This also includes any IT solution under ECOS evaluation.

3. ***Not currently cloud ready and cannot be made ready –*** IT solution is not currently cloud ready and it may or may not be possible for it to become cloud ready

4. ***Not currently cloud ready, can be and should be made cloud ready –*** the IT solution can technically be made cloud ready and there is a business case for doing so

5. ***Not currently cloud ready, can be but should not be made cloud ready –*** the IT solution can technically be made cloud ready and there is not a business case for doing so

6. ***Does not apply –*** PC deployed IT solution that included no server-based components