OIT Cloud First Policy 2012-13

Enabling Technology Solutions Efficiently, Effectively, and Elegantly

11/15/2012

Table of Contents

OIT Cloud First Policy 2012-13

Enabling Technology Solutions Efficiently, Effectively, and Elegantly

Executive Summary

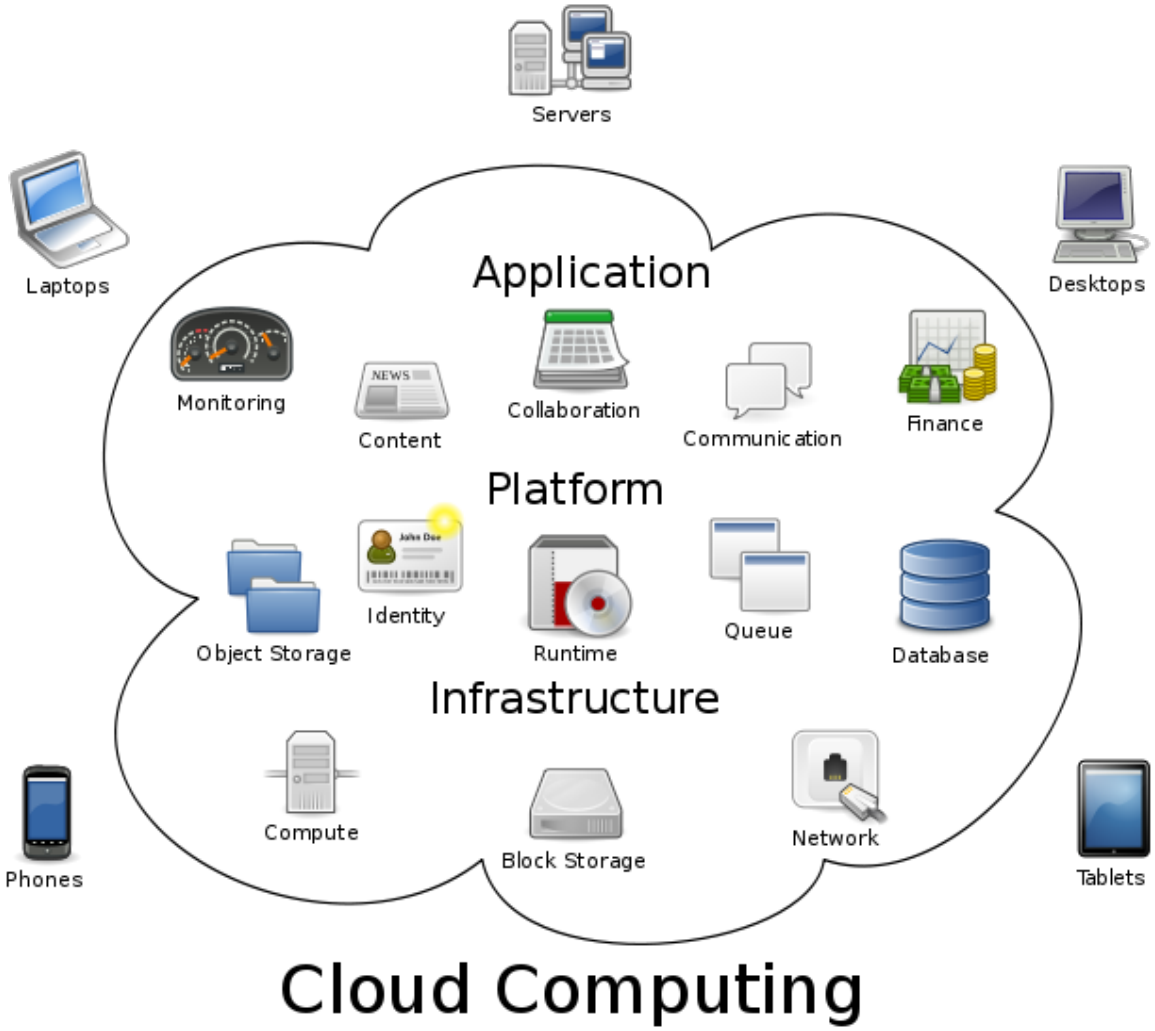
Cloud Computing is both a new and old technology. Old in that much of the technology has been around for years under other names: ASP, Virtualization, Grid. New in that the offerings have become sophisticated and allow everyone from start ups to governments to increase their technology efficiencies and reduce waste.

In the past, entities, especially governments, embraced the concept of private applications and infrastructure to maintain citizen security and privacy. Costs increased, as did resources, because maintenance was often manual and cumbersome. Even in today's current environment, many of the State's software applications are out of date and incompatible, often hampering business productivity. The cloud attempts to change that and remove some of the burdens that come with technology ownership. It shifts the onus of versions and change management to companies that claim it as a revenue stream and moves the rest of us away from maintenance toward Service Level Agreements and on demand technologies that can scale with our elastic demand. It also allows the State to leverage technology improvements and innovations that result from the business focus of cloud providers. Few would argue that the State of Colorado's focus is on service delivery to the citizens, not maintaining and managing a huge technical infrastructure and portfolio of applications. The cloud gives us the ability to focus on Citizen Engagement and the business of government.

Currently, there are pockets of cloud initiatives across the state, but no enterprise roadmap in which to work until now. The Compass: Enterprise Architecture 2011 – 2014 provides the overarching Enterprise Architecture for the State; while this document lays out the principles and decision criteria for employing "cloud first" services in specific instances and differentiates the different service and delivery models that may be appropriate for different application scenarios. Given the state of the industry, Colorado's IT infrastructure and footprint, and the opportunities that are available, Colorado is proceeding with a "cloud first" policy, mirroring the Federal government's cloud policy. To that end, Colorado is making a deliberate and explicit policy to "cloud first" services. We will proceed with the presumption that new services, applications and major revisions to existing applications will be supported in a cloud based environment first, unless there are substantive reasons why they should be hosted on the State's private infrastructure.

The Colorado Cloud Defined

At its heart, cloud technologies encompass a 'Pay as You Go' model, allowing the consumer of the resources to scale up and down at will. In reality, it has become a ubiquitous term that means many things.



*** Diagram from Wiki Commons file

Some key components of cloud technology include:

Elasticity: There is inherent scalability in the model

Flexible billing: Metering and resource usage combined with on-demand provisioning

Virtualization: Abstracted infrastructures encompass most cloud offerings

Service delivery:

Software as a Service

Platform as a Service

Infrastructure as a Service

Other 'as a Service'

Universal access: Location independence, resource democratization, resilience

Simplified management: Self service provisioning, accessible resources, upgrades automatic

Affordable resources: Dramatic reduction due to the 'pay as you go' model

Multi-tenancy: Public clouds can be used by multiple tenants

Service – level management: Reduced complexity

Delivery models for cloud offerings include:

Public Cloud

Hosted off-premise

Multi-tenant environment

Metered usage and billing

Self service provisioning

Private Cloud

Hosted, on-premise solution that scales to one organization through private network links. However, it can be a hosted solution off-premise, as long as the network infrastructure is private to one entity (in this case, the State of Colorado)

Multi-tenancy is minimized

Some solutions may not be 'pay as you go', since the capital is owned internally.

Security can be maximized, since the infrastructure is owned by the entity, not an external company.

Community Cloud

Group of organizations with a common set of requirements / objectives

Can allow an industry to advance in concert

Improves data and resource sharing among like organization / industries

Hybrid Cloud

Business units may have different business requirements that do not lend itself to one infrastructure

Applications may use different delivery points for applicable users.

Services may use different service delivery mechanisms.

Extension of internal systems leveraging public cloud systems

Colorado will use a hybrid model for the Enterprise as a whole. Certain components of the Enterprise Architecture may use one delivery mechanism only (such as email).

Cloud First - A Fundamental Shift around Infrastructure

Cloud computing outlines a fundamental shift for Colorado. The IT environment for the state has the same issues that many other organizations, including the federal government, have around its infrastructure:

Low asset utilization

Fragmented demand for resources

Duplicative systems

Difficulty managing the disparate systems

Long lead times for procurement

Aging infrastructure and application platforms and,

Resource constraints in staying current with technology developments

Cloud computing can address these inefficiencies and improve service delivery to citizens. It can further create a more agile environment, to promote innovation and a more proactive and scalable environment. Similar to the federal government cloud policy which created a Cloud First policy, Colorado is adopting the Cloud First policy and expects to transition most services to cloud computing over the next ten years. As part of this policy, Colorado will look to cloud provisioning first in new or expanded deployments of applications or services. Subsequently, existing applications will be evaluated for transitioning to a cloud platform. This will lead to greater efficiencies, but will also allow the State to take advantage of the research and development pursued by cloud service providers and the technological innovations that

result. Colorado state government does not have the resources for such research and should be focusing on the business needs of administering state government. The State will be particularly cognizant of and will anticipate ongoing reductions in cloud-based costs resulting from such innovations.

A decision rubric for identifying the appropriate cloud model for an application or services is presented at the end of this document. These decision frameworks will be reviewed quarterly.

Colorado Cloud Strategy Goals

The Colorado Cloud Strategy has four simple goals, which align with the overall Enterprise Architecture Roadmap for 2011-2014.

Reduce costs and redundancy
- Increase hardware usage
- Reduce data center footprint
- Recognize and reduce duplication in environments

Increase agility
- Simplify management of the environment
- Increase procurement throughput
- Improve scalability and elasticity

Continuously improve
- Take advantage of innovations in optimizing infrastructures for service delivery
- Rapidly adopt developments in applications

Reduce business, operational and security risk
- Ensure ongoing service levels for operations, security and monitoring
- Take advantage of specified time frames for incident resolution and refined processes for root cause analyses

Decision Framework for the Colorado Cloud Strategy

Delivery Models

Public

Government services revolving around communication and non-sensitive data dissemination are perfect candidates for public cloud offerings. In the current public cloud environment, risks around data security and privacy are still evolving. Extreme care should be taken when considering moving sensitive data (such as PII, HIPAA, FERPA, PCI) into a public cloud offering. The lines are blurring between public and private clouds. As a guideline, public clouds should be the ultimate goal for the state, since they offer the most in terms of economies of scale and cost efficiencies.

In general, a public cloud offering should either maximize or ensure that the following considerations are addressed:

Efficiency: The public offering should decrease the financial burden on the state and should be significantly more cost efficient than other delivery models.

Agility: The public offering should allow a faster time to market than other delivery models.

Security: The public offering should meet the security requirements for the initiative.

Technology Lifecycle: The public offering should replace hardware/software currently in use by the government that is at end of life.

The following are guidelines for storing data in the public cloud:

Data is stored in the United States.

Vendor must pass all CISO requirements OR no sensitive data is being stored.

Vendor's SLA states Colorado owns the data.

Legal jurisdiction is Colorado.

Change management processes (including data storage) are approved by CISO and CTO.

Bandwidth is available for the public delivery model into the government services and agencies.

Privacy Recommendations for Cloud Computing

A paper which highlights potential privacy risks agencies should consider as they migrate to cloud computing (CIO Council / http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx)

Private

Several flavors of private clouds are defined today. In general, private solutions may be more expensive than a public delivery model, but may offer additional security than a public cloud. The private cloud should maximize r ensure that the following are addressed:

Security: The private model should provide for better information security when there is a security risk with a public delivery model that cannot be overcome.

Technology Readiness: Bandwidth is available if the delivery model into the government services and agencies is from an external source.

Efficiency: The cost model should be 'on demand' or the hardware exists on premise.

Technology Life Cycle: The hardware should be vendor supported.

Virtual Private Clouds are becoming more common and these may be candidates for future offerings.

Hybrid

The enterprise for the State of Colorado will be based on a hybrid model, though much of the state's portfolio will be either public or private. Under certain circumstances, it will be useful to have a hybrid model, particularly when scaling is not linear. For example, during tax season peak times, it may be necessary to scale hardware from a private delivery model to encompass a public delivery model to ensure services. Under this scenario, a public cloud offering may be able to offload the additional temporary hardware requirements. This model should maximize the following:

Efficiency: The public offering should decrease the financial burden on the state, and it should be significantly more cost efficient to pursue a hybrid than add additional hardware to the private cloud.

Agility: The public offering should allow a faster time to market.

Security: The public offering should meet the security requirements for the initiative.

Technology Readiness: The hybrid solution should allow for the network/hardware/software changes required to take advantage of the environment.

Community

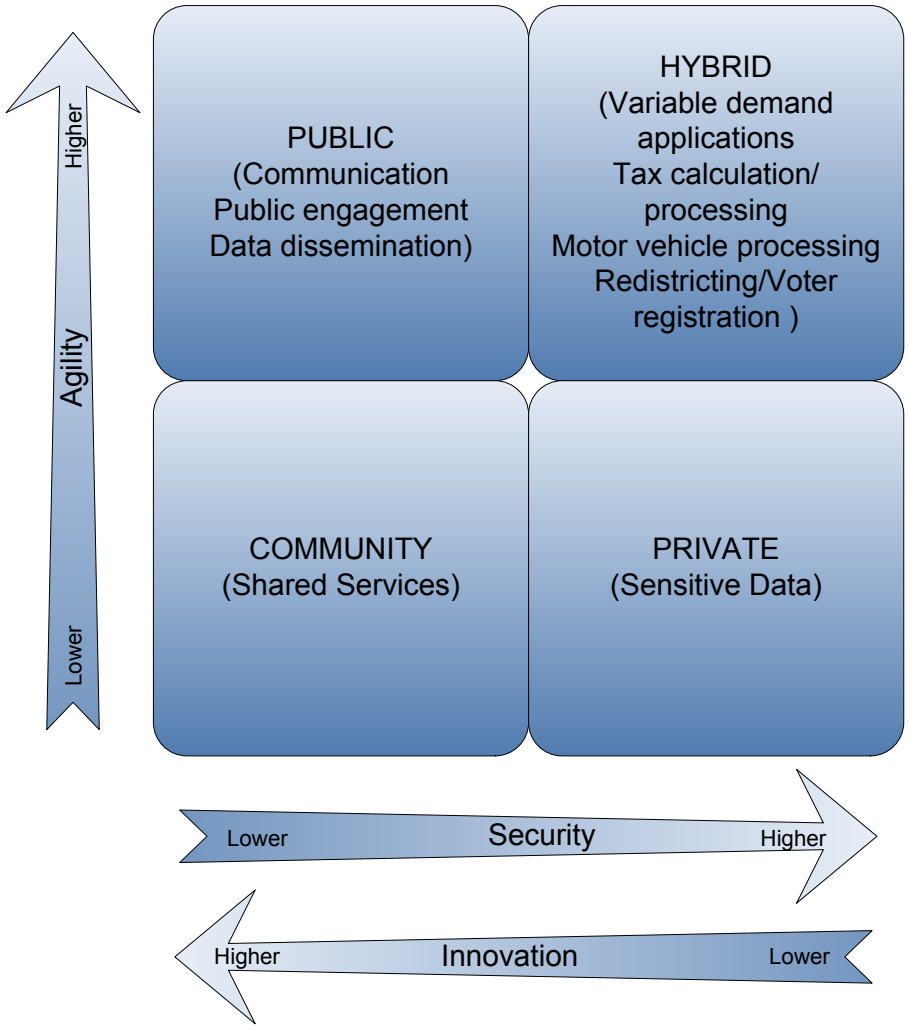
The state is currently pursuing community clouds with other states and should continue to pursue these types of delivery models as it makes sense. State and local governments may wish to pool resources in order to create economies of scale. In general, the community model should maximize the following:

Efficiency: The economies of scale should allow for a cost effective delivery model.

Innovation: The community offering should offer services not available outside of the community cloud.

Technical Readiness: Each entity within the community should share like processes and can support the delivery model.

These different platforms and how they relate to critical considerations for cloud computing may be depicted as:



Interoperability: Virtualization and Architectural Standards

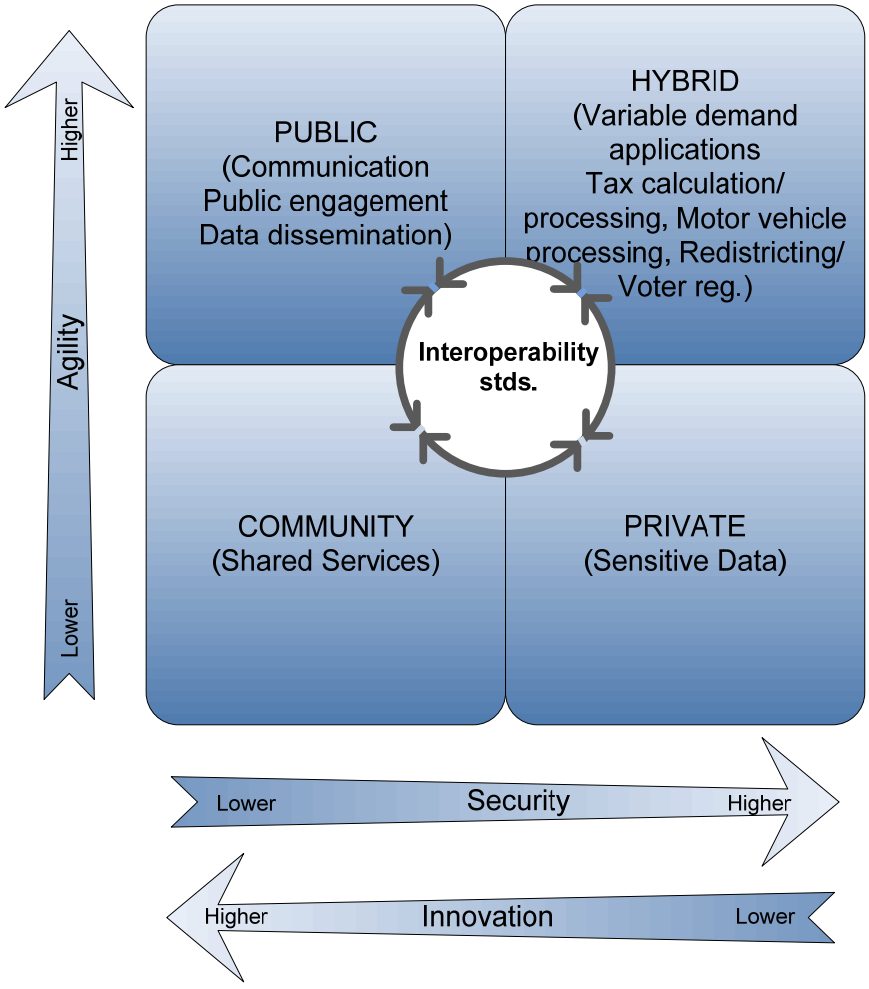
Core to the advantages of cloud computing is the opportunity for an organization to avoid the costs of managing a complex computing environment, if systems, networks, storage and virtual resources are adequately considered. Ultimately workloads or virtual machines should cross the boundaries between departmental data centers or silos to address the broad requirements of the State most efficiently. This will require an emphasis on standards and underlying platforms that promote interoperability. An emphasis on interoperability and related standards simplifies the management of cloud services and reduces the risk and effort associated with a commitment to cloud computing environments by supporting greater portability between delivery models.

An additional benefit of such interoperability is the ability to decompose complex applications into reusable services that may reside in any particular delivery model while the application is primarily

supported in another model. The end result is a common architecture which allows all assets and resources to be supported in the most effective environment and have a resonant value that is amplified across the entire organization and its services.

To achieve a consistent state of interoperability among its cloud services, cloud computing environments should conform to OIT standards related to virtualization and data center consolidation. When interoperability objectives have been achieved, computing environments will be more defined by the types of workloads and services that they support rather than location or ownership. In effect, the total computing environments of the state become defined by their services and workloads, rather than operational metrics, and effectively operate within a cohesive architecture that assigns uses to cloud delivery models.

The graphic below represents the central position of interoperability in the use of cloud resources:



Service Models

The state should pursue all service delivery models and stop relying on rich clients that are difficult to maintain. The delivery model will be combined with service models to create the most efficient and cost effective models. In all cases, security must be approved by the CISO.

Software as a Service

The Software as a Service (SaaS) service model should be pursued for all applications. Guidelines for choosing the vendor should include the following:

Identity Federation: As the state widens its portfolio to SaaS offerings, Single Sign On and Identity Federation will become more important.

Web Services and Open Platforms: The SaaS solutions should offer API's to move data in and out of the service. The platform should not be proprietary, but should offer an open platform for interoperability with other solutions.

Exit Strategy: Data should be available for download when a decision is made to leave the solution.

Platform as a Service

A Platform as a Service (PaaS) model is best when there is a high need for interoperability between disparate processes. These solutions offer ways to combine data and processes to create a business platform unavailable in the marketplace. These should include the following:

Identity Federation: As the state widens its portfolio to PaaS offerings, Single Sign On and Identity Federation will become more important. In addition too Identity Resolution which emables identity matching to resolve identity duplication across state systems.

Web Services and Open Platforms: The PaaS solutions should offer API's to move data in and out of the service. The platform should not be proprietary, but should offer an open platform for interoperability with other solutions.

Platform Integrations: The solution should offer multiple SaaS solutions that can be combined in multiple ways to create new business processes. For instance, a PaaS platform may offer a CRM SaaS solution that is easily integrated with a survey SaaS solution and a project management SaaS solution that can be combined without any proprietary code or integration solutions.

Exit Strategy: Data should be available for download when a decision is made to leave the solution.

Infrastructure as a Service

Virtualization of desktops is becoming increasingly useful as mobile devices become more ubiquitous. Customers want to access their applications and information anytime, anywhere. Please refer to the Enterprise Technology Roadmap for more information on virtualization and mobility.

All Other as a Service

New 'as a Services' a cropping up to address the needs of businesses and governments. Database as a Service, Identity as a Service, Security as a Service are all becoming feasible services to reduce costs and increase efficiencies. All will be scrutinized as the time comes for viability in the workplace. Each of the offerings should meet the goals outlined in the goals section above.

Security and Privacy Standards

The Colorado Cloud Strategy will adhere to all policies and standards set forth by the Chief Information Security Officer for the State of Colorado. Policies are found here:

http://www.colorado.gov/oit/security_policies

Information security standards are found here:

http://www.colorado.gov/oit/security_standards

The Government Data Advisory Board is responsible for enterprise privacy standards. These can be found here.

http://www.colorado.gov/cs/Satellite/OIT-EADG/CBON/1251579896288

Conclusion

There are numerous opportunities for Colorado to leverage cloud based technologies. It is important that the State's consumption of these services be governed and guided to avoid a simple replication of the current siloed IT situation in a cloud environment. OIT will take the leadership for this governance in the following ways:

Standards – The federal government is working on standards for cloud computing, many of which inform this document. OIT will document these standards and catalog other standards for various cloud deployments. Standards will increase flexibility and ability to leverage a variety of technologies to increase agility in the cloud.

Business use cases – OIT shall document business cases and provide guidance for developing business cases for potential cloud deployments. Federal government efforts may be leveraged. This documentation and guidance will facilitate planning for cloud use by helping agencies to consider specific objectives for their cloud deployments. In addition, it will provide background on financial or other benefits for those considering cloud computing. Ultimately, potential cloud initiatives should be included in department IT plans.

Procurement – OIT will take the lead on statewide price agreements for cloud services. This is being started with Colorado's participation in a four-state collaborative procurement through the Western States Contracting Alliance (WSCA) of cloud services to support geospatial information technologies. Agency procurements should be based on a centrally negotiated contract or price agreement to maximize cost efficiencies. In addition, such centrally negotiated contracts will include standard service level agreements that should be used unless there is a specific need.

Monitoring – OIT will provide guidance for and record results of monitoring cloud service to ensure anticipated benefits are being realized and developing an ongoing record of services and service providers that perform well.

The following table presents decision points for "opting out" of the cloud first paradigm. It applies to new applications or services or major developments or enhancements to existing ones and helps identify the appropriate service and delivery models.

IaaS	PaaS	SaaS
1. Does application or service include information classified as Level 2 or above? A. No: Public or Community Cloud B. Level 2: Public or Hybrid Cloud may be used with sufficient access constraints and security policies. C. Level 3 or 4: Private Cloud	1. Does application or service include information classified as Level 2 or above? A. No: Public or Community Cloud B. Level 2: Public or Hybrid Cloud may be used with sufficient access constraints and security policies. C. Level 3 or 4: Private Cloud	1. Does application or service include information classified as Level 2 or above? A. No: Public or Community Cloud B. Level 2: Public or Hybrid Cloud may be used with sufficient access constraints and security policies. C. Level 3 or 4: Private Cloud
2. Is application or service continuation of application currently hosted in-house with no significant enhancements or amendments and hardware is not near End of Life? A. No: Public or Community Cloud B. Yes: In-house	2. Is application or service continuation of application currently hosted in-house with no significant enhancements or amendments and hardware is not near End of Life? A. No: Public or Community Cloud B. Yes: In-house	2. Is application or service continuation of application currently hosted in-house with no significant enhancements or amendments and hardware is not near End of Life? A. No: Public or Community Cloud. B. Yes: In-house
3. Does application or service require regular up or downloads of large amounts of data or is there workflow that requires using in-house infratructure that would pose a major security risk? A. Yes: In-house or Private Cloud B. No: Public, Community or Hybrid Cloud.	3. Does workflow require in-house infrastructure? A. Yes: In-house or Private Cloud. B. No: Public or Community Cloud. 4. Does application or service require regular up or downloads of large amounts of data? A. Yes: In-house or Private Cloud B. No: Public, Community or Hybrid Cloud.	3. Does workflow require in-house infrastructure? A. Yes: In-house or Private Cloud. B. No: Public or Community Cloud. 4. Does application or service require regular up or downloads of large amounts of data? A. Yes: In-house or Private Cloud. B. No: Public or Community Cloud.