Multi-Cloud and Hybrid Cloud Guide

September 3, 2021

Office of Information Integrity and Access

General Services Administration
Office of Government-wide Policy

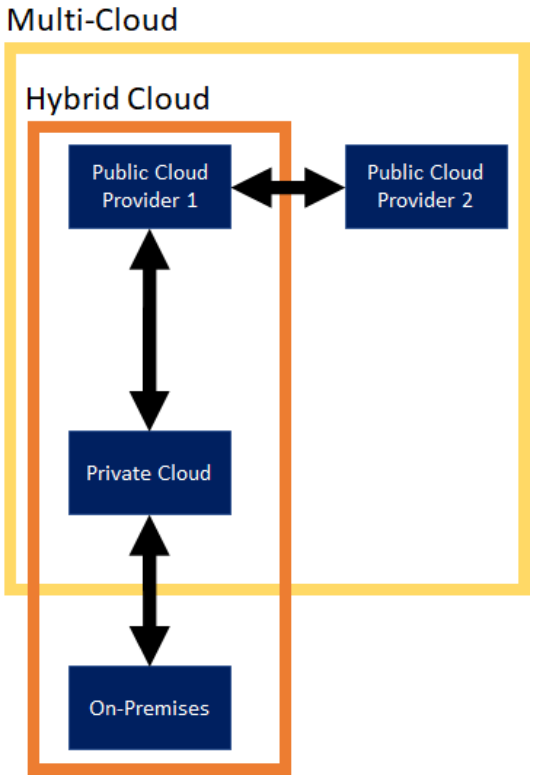
Table of Contents

Executive Summary

As cloud computing environments expand and become more diverse, agencies face an ever-growing number of cloud services, offerings, and options. Agencies will need informed strategies to understand, anticipate, rationalize, and optimize major cloud architecture decisions.

Key considerations in these decisions are if and how agencies integrate on-premises infrastructure into their cloud environments. The difference between multi-cloud and hybrid cloud architectures is the absence or presence of on-premises infrastructure, respectively (**Figure 1**). This distinction has implications on cost effectiveness, manageability, performance, reliability, security and privacy, and the IT workforce.

Figure 1. *Hybrid cloud architecture includes on-premises infrastructure, while multi-cloud architecture does not. Furthermore, unlike hybrid cloud solutions, multi-cloud solutions generally include more than one public Cloud Service Provider (CSP).*



This Multi-Cloud and Hybrid Cloud Guide is intended to help your agency navigate these decisions. It brings together the most relevant information on different cloud architectures, compares the advantages and disadvantages of each, and walks your agency through important considerations pertaining to an Infrastructure as a Service (IaaS) cloud solution.

Introduction

Intended Audience

The intended audience for this document includes Information Technology (IT) infrastructure and operations leaders, enterprise architects, and IT strategy and policy analysts at both the agency and component level.

Purpose

As cloud computing environments expand and become more diverse, agencies face an ever-growing number of cloud services, offerings, and options. Informed strategy is needed to understand, anticipate, rationalize, and optimize major cloud architecture decisions. The purpose of this guide is to:

- Present the most relevant information on different cloud architectures (both multi-cloud and hybrid cloud), and compare the advantages and disadvantages of each.
- Discuss important considerations in the selection, adoption, and management of an Infrastructure as a Service (IaaS) cloud solution.

Structure

This document is organized into four primary sections:

- **Cloud Architectures:** Defines and characterizes multi-cloud and hybrid cloud architectures.
- **Management:** Describes management best practices, management shifts to enable use of multi-cloud and hybrid cloud architectures, and Cloud Management Platforms (CMPs).
- **Analysis of Alternatives:** Assesses multi-cloud and hybrid cloud architectures against defined evaluative criteria.
- **Determine Your IaaS Cloud Solution:** Provides top issues to consider when selecting the best fit cloud architecture for your broader IT strategy.

Cloud Architectures

Multi-Cloud Architecture

Overview

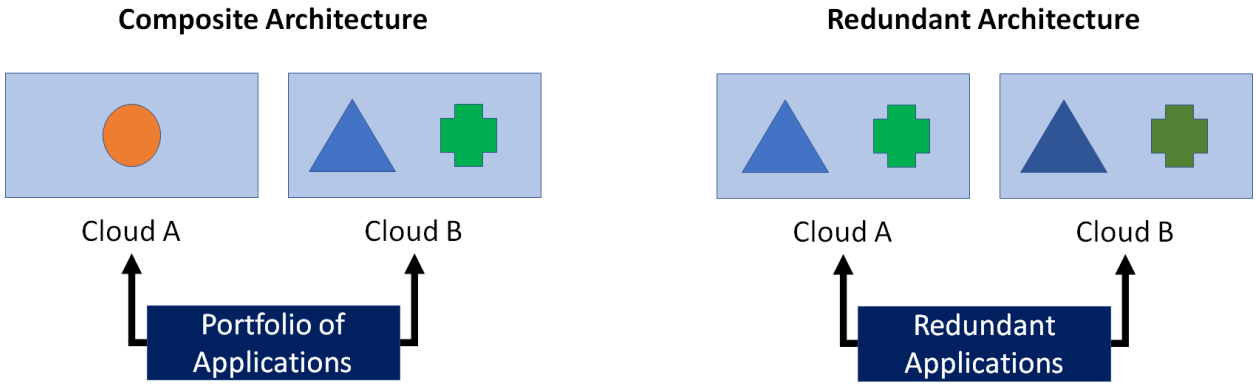
Multi-cloud architecture is the explicit use of the same type of cloud services from multiple IaaS CSPs. It is a broad term, sometimes denoting associated multi-cloud management/operations or non-integrated use of multiple clouds.[1] The term may encompass all-private clouds, all-public clouds, or a combination of both.[2] While it may include a mix of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) cloud solutions, this guide focuses on IaaS solutions.

While the term is broad, in this document, multi-cloud refers to the deliberate integration of services from multiple CSPs. A collection of cloud services that serve an enterprise but were created on an ad-hoc or patchwork basis is not considered as true multi-cloud architecture.

Types

There are two types of multi-cloud architecture, **composite architecture** and **redundant architecture**, as shown in **Figure 2**.[3] In composite architecture, a portfolio of applications is distributed across two or more CSPs. It is preferred when performance is the key

Figure 2. *Diagrams of composite and redundant multi-cloud architecture.*



[1] Gartner. (2020, January 15). *IT Leaders' Strategy Deck: Multicloud and Hybrid Cloud* [PowerPoint slides]. Gartner. https://www.gartner.com/document/3979621
[2] If an application on a private cloud is deemed mission-critical by a continuity of operations plan, then that private cloud should be housed in an agency-controlled, CSP-based Virtual Private Cloud (VPC). Please refer directly to CSP information (not referenced in this document) for exhaustive lists of recommended specifications and capabilities.
[3] Gartner. (2020, January 15). *IT Leaders' Strategy Deck: Multicloud and Hybrid Cloud* [PowerPoint slides]. Gartner. https://www.gartner.com/document/3979621

consideration. Meanwhile, redundant architecture contains two or more instances of the same application, and allows for one cloud to take over when another fails (i.e., a failover). It is preferred when availability and resilience of the application is a key consideration. In redundant multi-cloud architecture, implementation of an application from one cloud to another is not an exact replication. Thus, while Cloud A and B share the same shapes, they are not identical (in this instance, indicated by a darker shade of green in Cloud B).

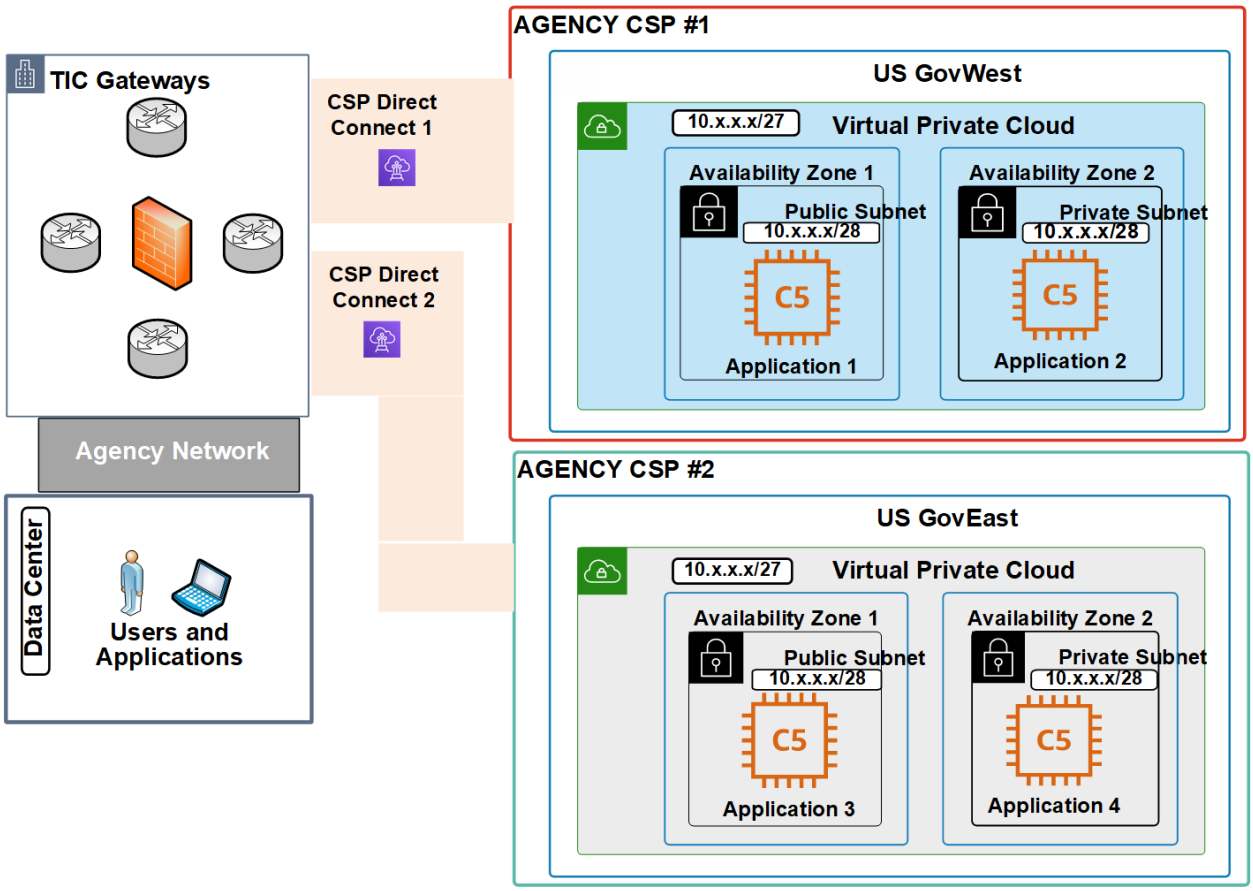
Deployments of redundant multi-cloud architecture can occur in the following ways.[4]

- **Continuously replicated:** the same application runs on two or more IaaS CSPs.
- **One-time placement:** an application can be moved between IaaS CSPs, but it operates on only one of them at a time.

Generic Use Case

Figure 3 illustrates a generic use case for multi-cloud architecture. First, an on-premises data center is connected to an agency network. Then, this network is connected to two

Figure 3. *Generic use case of multi-cloud architecture.*



[4] Gartner. (2020, January 15). *IT Leaders' Strategy Deck: Multicloud and Hybrid Cloud* [PowerPoint slides]. Gartner. https://www.gartner.com/document/3979621

CSPs through Trusted Internet Connection (TIC) gateways and, later, CSP Direct Connect 1 and 2. CSP Direct Connect 1 and 2 must correspond to Agency CSP #1 and #2, respectively.

Agency CSP #1 and #2 each house VPCs with different applications. The VPC from Agency CSP #1 (US GovWest) hosts Application 1 and 2, while the VPC from Agency CSP #2 (US GovEast) hosts Application 3 and 4. Within each VPC, one application (1 and 3) is deployed on a public subnet, and the other (2 and 4) is deployed on a private subnet. The applications on the public subnet are on a public cloud and are public facing, while those on the private subnet remain on a private cloud and are internally facing. As displayed in **Figure 3**, the deployment of individual applications across public and private clouds demonstrates composite multi-cloud architecture.

SWOT Analysis

Table 1. *SWOT analysis of multi-cloud architecture.*

	Helpful	Harmful
Internal (Agency)	**Strengths** • Leverages best-of-market innovations and capabilities, and mitigates risk of vendor lock-in. • Increases agility, scalability, and flexibility. • Prepares agencies to define and manage enterprise architecture. • Potentially decreases the total cost of ownership (TCO). • Less risk associated with cloud-agnostic contracts.	**Weaknesses** • Increases in recruiting, hiring and training costs. • Mounting managerial burden due to an increase in integration-related complexity. • Operational and cost inefficiency. • Slower data transmission between public and private cloud environments due to network constraints.
External	**Opportunities** • Provides an integrated experience for users. • Prevents loss and corruption of data. • Increased competition and better pricing. • Improves resilience and service delivery.	**Threats** • Increases the attack surface due to an increase in complexity.

The advantages and disadvantages of multi-cloud architecture are analyzed using the SWOT framework (which stands for strengths, weaknesses, opportunities, and threats). Strengths and weaknesses originate within the agency using multi-cloud architecture, while opportunities and threats originate outside of the agency. The findings of the SWOT analysis are summarized in **Table 1** and are laid out in the subsections that follow.

Strengths

- **Leverages best-of-market innovations and capabilities:** A potential risk of single cloud or single CSP environments is vendor lock-in. The involvement of multiple CSPs mitigates this risk, and agencies can better align specific requirements with the best available services and products.
- **Increases agility, scalability, and flexibility:** Although more choices can increase complexity, a strong multi-cloud architecture allows agencies the flexibility and agility to meet significant demand and scaling needs within their existing architecture. Workload mobility is significantly increased in a well-functioning multi-cloud environment.[5]
- **Prepares agencies to define and manage enterprise architecture:** The process of adopting multi-cloud enterprise architecture can help agencies evaluate and improve their current management practices and application portfolio. To bolster these efforts, agencies should strongly consider using The Application Rationalization Playbook, which provides a guide on how to strategically determine which applications should be migrated to the cloud and which should be retired.
- **Potentially decreases the total cost of ownership (TCO):** The TCO for multi-cloud infrastructure may be lower than for on-premises infrastructure.[6] Agencies only pay for the services that they need to run applications or handle data, rather than paying for all the hardware and software costs associated with on-premises infrastructure.
- **Less risk associated with cloud-agnostic contracts:** Use of cloud-agnostic contracts across multiple CSPs helps agencies avoid legal and financial risks typically associated with outsourcing cloud services to third parties. In turn, agencies benefit from easier use of open-source technologies like Kubernetes to enhance portability.

Weaknesses

- **Increased recruiting, hiring and training costs:** There is an increased need for the IT workforce to understand and adopt knowledge of multiple tools, providers, and systems. Often, an agency's existing IT workforce does not meet the new skill requirements, raising training, recruiting, and hiring costs for the organization. Agencies must also account for an increase in training costs for teams and

[5] In this guide, a workload is synonymous with an application. Thus, workload mobility refers to the movement of applications and corresponding data from one environment to another (e.g., from one cloud to another, or from a cloud to on-premises infrastructure).
[6] Importantly, the TCO for multi-cloud infrastructure could far exceed that for on-premises infrastructure for agencies that are mature in their cloud adoption and use CPU- and memory-intensive applications (e.g., training machine learning models).

individuals directly responsible for the cloud service and periphery teams and individuals who support it.

- **Mounting managerial burden due to an increase in integration-related complexity:** With the increasing number of providers, tools, and applications being added for different purposes, organizations struggle to integrate the necessary tools, creating silos throughout their IT environments. This creates a managerial burden that could emerge in a variety of different ways across the organization, including:
    - Management of different CSP networks, firewall rules, and security rules.
    - Configuration of user VPN access and Direct Connect access.
    - Provisioning new accounts and environments.
    - The application framework process.
    - Use of redundant security toolsets.
    - The build automation process, which may require longer testing cycles and more updates to automation processes.
- **Operational and cost inefficiency:** As the cloud environment grows, processes emerge independently of one another and create resource and monetary waste for the organization. Consequently, management may encounter difficulty in mapping and overseeing these processes. For example, independent management of two or more CSP cost and billing models may lead to suboptimal cost efficiency.
- **Slower data transmission between public and private cloud environments due to network constraints:** Network constraints can cause data transmission latency. As a result, networks can slow data transmission between public and private cloud environments.

Opportunities

- **Provides an integrated user experience:** If an agency responds favorably to the managerial and operational challenges noted above, the result may be an integrated experience not only for IT staff, but also for non-IT staff and users of public facing services provided by the agency.
- **Prevents loss and corruption of data:** Separation of key management services from applications leveraging those services can prevent potential data loss and data corruption associated with the compromise of one IaaS environment.
- **Lower prices as a result of increased competition:** As more vendors enter the federal marketplace and seek business with a given agency, they may lower their rates in order to remain competitive, resulting in cost savings for that agency.

- **Improves resilience and service delivery:** When an emergency occurs, the heterogeneity of multi-cloud architecture can help protect mission-critical applications and data via redundant backup and recovery capabilities. In a multi-cloud approach where services are duplicated, an agency is insulated from vendor-specific outages. While not common, vendor-specific outages can have a major impact on delivery of government services.[7]

Threats

- **Increases the attack surface due to an increase in complexity:** Greater complexity associated with management across multiple IaaS providers (including identity management) increases the risk of security gaps. Additionally, mitigation of these gaps often poses a challenge because risk mitigation procedures vary across CSPs.

[7] CloudHarmony provides a real-time tracker of CSP issues and outages.

Hybrid Cloud Architecture

Overview

In this guide, **hybrid cloud architecture** is defined as the deliberate integration of public cloud, private cloud, and on-premises infrastructure. Though it is often mentioned as a form of multi-cloud, multi-cloud does not use on-premises IT infrastructure.

Types

Composite architecture and **redundant architecture** also exist in hybrid cloud. Composite architecture contains a portfolio of applications distributed across public CSPs, private CSPs, and on-premises infrastructure. As in multi-cloud, composite architecture is preferred in hybrid cloud when performance is the key consideration. In contrast, redundant architecture contains copies of the same application across public CSPs, private CSPs, and on-premises infrastructure, and offers failover capability when an instance fails. Redundant architecture is the favored approach in hybrid cloud when availability and resilience of the application is a key consideration. Please see **Figure 4** and **Figure 5** for illustrations of composite and redundant architecture, respectively.

As shown by the illustration of redundant hybrid cloud architecture in **Figure 5**, implementation of an application—from one cloud to another or to on-premises infrastructure—is not an exact replication. While the applications in Cloud A, Cloud B, and On-Premises share the same shapes, they are not identical. To show that they differ, the

Figure 4. *Structure of composite hybrid cloud architecture.*

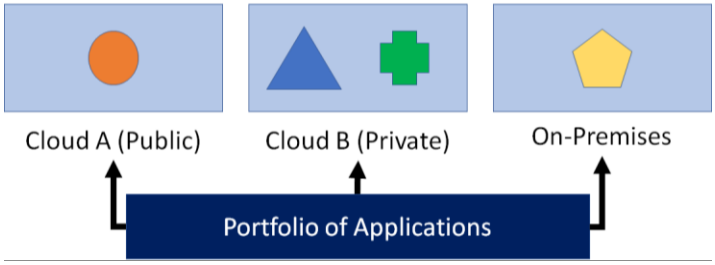
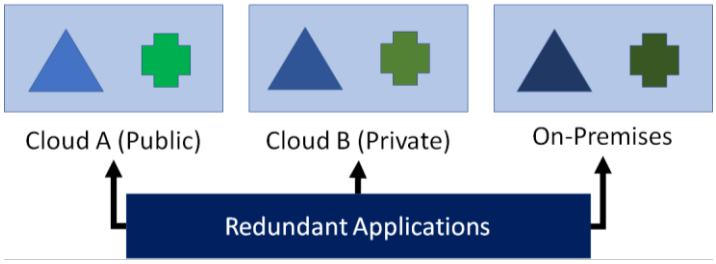


Figure 5. *Structure of redundant hybrid cloud architecture.*



shapes in Cloud B and in On-Premises become progressively darker. Importantly, applications in redundant hybrid cloud architecture are generally replicated in two but not all three places at a given time.

Deployments of redundant hybrid cloud architecture can occur in the following ways.

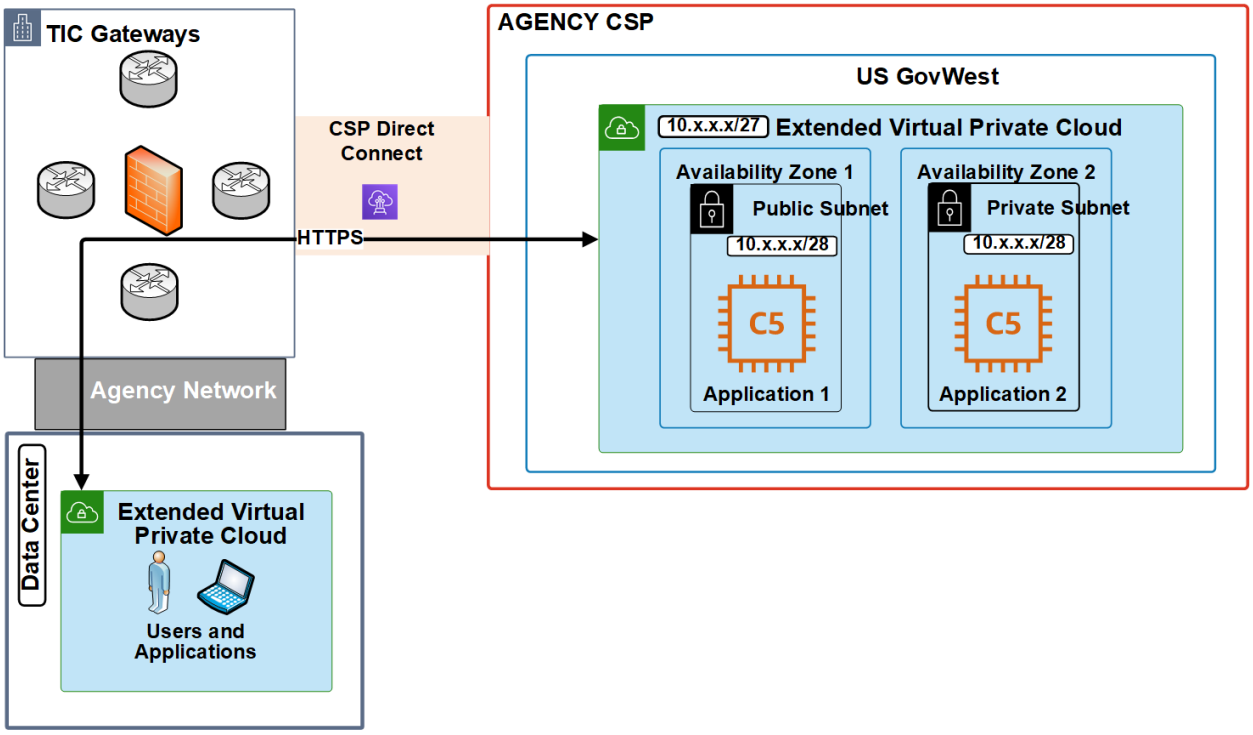
- **Continuously replicated:** the same applications are supported by two or more CSPs and/or by on-premises infrastructure.
- **One-time placement:** an application is supported by two CSPs and by on-premises infrastructure, but it runs on one location at a time with the other locations on stand-by in case of a failover.

Generic Use Case

Figure 6 shows a generic use case for hybrid cloud architecture. In the figure, an on-premises data center is connected to the agency CSP via the agency network, Trusted TIC Gateway, and CSP Direct Connect. The extended VPC allows for integration of on-premise applications to CSP services.

The extended VPC (US GovWest, in this example) hosts Application 1 and 2. Application 1, on the public subnet, is on a public cloud and is public facing, while Application 2, on the private subnet, remains on a private cloud and is internally facing. The combination of public and private clouds with on-premises infrastructure is the configuration of hybrid cloud architecture.

Figure 6. *Generic use case of hybrid-cloud architecture.*



SWOT Analysis

The SWOT analysis of hybrid cloud architecture is summarized in **Table 2** and discussed in detail in the subsections that follow.

Table 2. *SWOT analysis of hybrid cloud architecture.*

	Helpful	Harmful
Internal (Agency)	**Strengths** ● Retains legacy applications. ● Retains sensitive applications and data on-premises. ● Provides an integrated experience for customers. ● Leverages functional advantages from a combination of public and private CSPs. ● Encourages late adopters of cloud technology. ● Potentially decreases the TCO.	**Weaknesses** ● Increases in hiring and training costs. ● Available workforce with expertise is still limited. ● Networks can impact data transmission between public and private cloud environments.
External	**Opportunities** ● Managed public cloud service extension to the edge from public cloud providers. ● Cloud management platforms (CMPs) maturing and improving management burden. ● Improves resilience and service delivery.	**Threats** ● Increases the attack surface due to an increase in complexity. ● Edge private cloud services are still maturing

Strengths

- **Keeps legacy applications on-premises:** For many agencies, the main appeal of hybrid cloud architecture is the retention of legacy applications on-premises, while still providing an opportunity to modernize the rest of their IT infrastructure and attain the benefits of cloud computing.
- **Keeps sensitive applications and data on-premises:** If an agency's risk tolerance prohibits storage of sensitive data on the cloud, then it has the option of housing them on-premises while using the cloud to store non-sensitive data.[8]

[8] Agencies should note that they may achieve the same or greater security in the cloud, especially as more CSPs use Federal Information Security Modernization Act (FISMA) High cybersecurity controls.

- **Provides an integrated experience for customers:** With a cloud management platform (CMP) suitable for hybrid cloud architecture, users are able to effectively and simultaneously manage public and private cloud infrastructure, in addition to on-premises infrastructure.
- **Leverages functional advantages from a combination of public and private CSPs:** Commonly, agencies seek to attain functional advantages from a combination of public and private CSPs. While a public cloud may require no maintenance and offer almost unlimited scalability, a private cloud may provide more privacy controls and security. In the process of seeking these functional advantages, they will also avoid vendor lock-in.
- **Encourages late adopters of cloud technology:** Agencies whose IT infrastructure is still on-premises may begin their cloud journey by moving progressively more applications to the cloud, while retaining their on-premises infrastructure.
- **Potentially decreases the TCO:** The TCO for hybrid cloud infrastructure may be lower than the TCO for on-premises infrastructure alone. Agencies only pay for the cloud services they need, while incurring far lower costs associated with on-premises infrastructure.[9] It is important to recognize that costs can only be lower if the hosted environment is optimized and services are automated to the greatest extent possible.

Weaknesses

- **Increased hiring and training costs:** As with multi-cloud architecture, hybrid cloud architecture requires the IT workforce to become proficient with multiple tools, providers, and systems. Often, an agency's existing IT workforce does not have the required skills to manage the new architecture, raising training and hiring costs for the organization.
- **Available workforce with expertise is still limited:** Management of hybrid cloud architecture is complex and, consequently, there is a limited pool of cloud architects with the requisite skills. While training can expand that pool, it is often very costly for individual agencies.
- **Networks can slow data transmission between public and private cloud environments:** Network constraints can cause data transmission latency.

Agencies must make that determination individually, as part of their larger risk management process.

[9] As with multi-cloud infrastructure, the TCO for hybrid cloud infrastructure could far exceed that for on-premises infrastructure for agencies that are mature in their cloud adoption and use CPU- and memory-intensive applications (e.g., training machine learning models).

Opportunities

- **Managed public cloud service extension to the edge from public cloud providers:** Some public CSPs now offer edge computing capabilities, which can reduce costs and increase efficiency. Agencies using hybrid cloud architecture can leverage this technology, while still using the private environment to store sensitive applications and data, for example.
- **CMPs maturing and improving management burden:** Recent advancements in CMPs now allow users to effectively manage hybrid cloud architecture. As the technology matures, agencies can anticipate a progressively reduced burden to manage both off- and on-premises IT infrastructure.
- **Improves resilience and service delivery:** In an emergency, the heterogeneity of hybrid cloud architecture, like that of multi-cloud architecture, can protect mission-critical applications and data via redundant backup and recovery capabilities. In a hybrid cloud approach where services are duplicated, an agency is insulated from vendor-specific outages. While not common, vendor-specific outages can have a major impact on delivery of government services.[10]

Threats

- **Increased attack surface due to an increase in complexity:** An increase in complexity means an increased attack surface, which is comparatively greater than in multi-cloud due to the presence of on-premises infrastructure. If architecture is configured incorrectly, security risks increase. To protect against security threats, agencies need service visibility and strong automated governance controls.
- **Edge private cloud services are still maturing:** Using edge cloud services, agencies can circumvent the need to build their own cloud environment. Yet, despite new commercial offerings, the technology is unproven and agencies considering it should be aware of the associated operational, financial, and regulatory risks.

[10] CloudHarmony provides a real-time tracker of CSP issues and outages.

Management

Management Best Practices

Any multi-cloud or hybrid cloud implementation should centralize core infrastructure services needed to operate an IT environment while distributing the business functionality among CSPs. For instance, core security services such as identity management and key management should not be re-implemented in separate CSPs, whenever possible. Agencies must determine which services can and should be centralized, while also leveraging native toolsets from the CSP that offer superior functionality in comparison to third party solutions.

Organizations that choose to adopt multi-cloud or hybrid cloud solutions can recognize significant benefits, but there are still risks and complexities involved in the adoption process. To realize the many benefits, it is critical that agencies employ best practices for the adoption process. Gartner recommends three management best practices for successful adoption.[11]

1. Organizations should recognize that both multi-cloud and hybrid cloud solutions are only elements of a larger enterprise-wide cloud strategy. Considering these options as part of a larger cloud strategy (and, by extension, agency strategic planning) is critical to ensure that all elements of the IT infrastructure work together to optimize efficiencies and effectiveness.

2. Strategic architectural choices can help balance complexity concerns with the expected benefits of a multi-cloud or hybrid cloud environment. Complexity concerns generally arise from the below areas.

    - **Integration:** from receiving services to integrating them.
    - **Skills:** overlapping engineering practices and knowledge of tools/providers.
    - **Tools and processes:** increasing difficulty to manage and map.

    Furthermore, skills, integration, and tools complexity have "knock-on effects." For instance, an increase in the complexity of the skills required can increase workforce costs due to training needs, a need to increase compensation to attract and retain talent with the proper skills, or simply a need to increase the number of employees.

3. Organizations must be willing to replace standard operating procedures and management practices (e.g., "this is how we have always done it") with a broader

[11] Gartner. (2020, January 15). *IT Leaders' Strategy Deck: Multicloud and Hybrid Cloud* [PowerPoint slides]. Gartner. https://www.gartner.com/document/3979621

management approach that prioritizes engineering and incorporates the management shifts described in the next section.

Management Shifts

For an effective transition to multi-cloud or hybrid cloud architecture, agencies benefit from shifts in IT management approach in the following areas.[12]

- **Cloud service management:** from independent teams to centralized management.
- **Customer and request interface approaches:** from manual to automated service fulfillment.
- **Cloud governance controls and policies:** from "guidelines" and retrospective controls to guardrails and preventive controls.
- **Cloud operations:** from siloed to shared processes.
- **Growing a more versatile workforce:** from specialized to cross-silo skills.

Cloud Service Management

As agencies transition to a multi-cloud or hybrid cloud architecture, they benefit from a shift away from independent teams, which use a diversity of processes and technologies, and towards centralized management of resources and standardized processes (**Table 3**). While independent teams offer a wide array of options for developers and users, and help agencies circumvent political and process-related impediments, they also create inconsistencies in governance and contracting. Centralized management fixes these inconsistencies by facilitating prescriptive, top-down governance and harmonizing procurement and acquisition activities. Additionally, through a centrally managed approach, agencies can automate provisioning across different cloud environments, allowing them to dynamically match cloud resources according to demand.

Table 3. *Management shifts from independent teams to centralized management.*

Independent Teams	Centralized Management
• Gives a wide array of options for developers and users. • Streamlines execution and helps prevent IT bottlenecks. • Helps avoid political/hierarchical impediments.	• Facilitates prescriptive, top-down governance. • Harmonizes procurement and acquisition activities. • Easier to automate provisioning across different cloud environments.

[12] Gartner. (2020, January 15). *IT Leaders' Strategy Deck: Multicloud and Hybrid Cloud* [PowerPoint slides]. Gartner. https://www.gartner.com/document/3979621

Cloud and Request Interface Approaches

A transition to multi-cloud or hybrid cloud architecture is facilitated by a corresponding shift in agencies' approach to interacting with customers and addressing requests. Broadly speaking, this shift decreases agencies' use of manual service fulfillment, in which infrastructure and operations staff respond to customer requests, and increases their use of automated service fulfillment, in which automated services respond to customer requests (**Table 4**). Users benefit from manual service fulfillment because they can lower the skills barriers and repeatable tasks needed to make requests. However, in multi-cloud and hybrid cloud, agencies should pursue automated service fulfillment to leverage both the substantial increases in agility and improvements in functionality for users and developers. Automated service fulfillment also provides a way for agencies to lessen their direct control over the user experience, which becomes impractical in highly scalable cloud environments.

Table 4. *Management shifts from manual to automated service fulfillment.*

Manual Service Fulfillment	Automated Service Fulfillment
• Ensures direct control over user experience. • Lowers skills barriers and repeatable tasks necessary to make requests.	• Substantially increases agility. • Improves functionality for users and developers.

Cloud Governance Controls and Policies

In pursuing multi-cloud or hybrid cloud architecture, agencies benefit from a shift in cloud governance, from guidelines and retrospective controls to guardrails and preventive controls (**Table 5**).[13] Though requiring less effort and skill to execute, guidelines and retrospective controls suffer from a lack of specificity to actual code and tools and a lack of mechanisms to enforce governance compliance. Guardrails and preventive controls resolve these issues because they establish mechanisms to instantly enforce compliance to code and tools. Furthermore, agencies that use guardrails and preventive controls generally see a decreased risk of cybersecurity breaches and can better control costs. Thus, relative to guidelines and retrospective controls, guardrails and preventive controls ease the managerial burden on agencies.

[13] Guidelines and retrospective controls refer to a governance framework that uses remediative and retroactive processes to guide how cloud computing services are used. In contrast, guardrails and preventive controls take a proactive, high-level, and often automated approach to cloud governance.

Table 5. *Management shifts from "guidelines" and retrospective controls to guardrails and preventive controls.*

Guidelines and Retrospective Controls	Guardrails and Preventive Controls
• Suffer from a lack of specificity to actual code and tools. • Suffer from a lack of mechanisms to enforce governance compliance. • Require less effort and skill to execute.	• Establish mechanisms to instantly enforce compliance to code and tools. • Decrease the risk of cybersecurity breaches. • Can better control costs.

Cloud Operations

To manage multi-cloud or hybrid cloud architecture efficiently and effectively, agencies are encouraged to use centralized visibility and controls as the foundation for their cloud operations (**Table 6**). In practical terms, use of centralized visibility and controls requires a shift away from processes that are specific to on-premises infrastructure or different clouds (i.e., distributed management), and towards processes shared across IT environments. While siloed processes generally correspond with more service offerings, teams that are more agile, and faster implementation, at the same time, they lead to the fragmentation of skill sets and prevent operations managers from gleaning agency-level insights. Agencies that transition to shared processes can consistently monitor and control operations across a cloud environment, as well as implement cross-platform applications. Furthermore, by consolidating skills sets and tools, agencies that pursue shared processes benefit from greater engagement not just among developers, but also among non-IT staff.

Table 6. *Management shifts from siloed processes to shared processes.*

Distributed Management	Centralized Visibility and Controls
• Corresponds with more service offerings, teams that are more agile, and faster implementation. • Leads to the fragmentation of skill sets. • Prevents operations managers from gleaning agency-level insights.	• Can consistently monitor and control operations across a cloud environment. • Can implement cross-platform applications. • Encourage more engagement among IT and non-IT staff.

Workforce Versatility

A more versatile workforce is critical for agencies considering multi-cloud or hybrid cloud architecture. Agencies may grow a more versatile workforce through a variety of short-term (i.e., weeks to months) and long-term (i.e., months to years) strategies (**Table 7**). Across this journey, agencies pursue a workforce that relies less on specialized skills and more on cross-silo collaboration and innovation. Short-term strategies include hiring or contracting to fill skills gaps, rotating staff through low-risk, experiential learning opportunities, and promoting cross-silo workshops to foster innovation. Long-term strategies include creating employee incentives for skills diversification, identifying and

communicating career paths for roles in high demand, and incorporating cross-silo learning activities into employee development.

Table 7. *Short- and long-term management shifts from specialized skills to cross-silo skills.*

Short-Term Strategies	Long-Term Strategies
• Hiring or contracting to fill skills gaps. • Rotating staff through low-risk, experiential learning opportunities. • Promoting cross-silo workshops to foster innovation.	• Creating employee incentives for skills diversification. • Identifying and communicating career paths for roles in high demand. • Incorporating cross-silo learning activities into employee development.

Cloud Management Platforms

CMPs integrate public, private, and, in some cases, on-premises management into a unified software tool. Therefore, some CMPs may be used to manage hybrid cloud architecture in addition to multi-cloud architecture. They generally focus on the management of IaaS components: networking, storage, servers, and virtual machines.

CMPs share key characteristics that help agencies manage the ever-growing complexity of cloud and hybrid IT environments. Perhaps the most critical component of the environment is automation. A typical CMP can centralize routine cloud automation tasks from workload optimization (via autoscaling) to provisioning in support of the DevOps lifecycle. CMPs also help agencies control costs by matching the size of cloud instances according to workload requirements (i.e., rightsizing). Further, security and compliance activities are streamlined through CMPs. For instance: encryption, role-based access control, and user authentication and authorization can all be managed across an entire multi-cloud or hybrid cloud architecture (i.e., across a combination of public CSPs, private cloud, and on-premises infrastructure).

CMPs have broad appeal because they offer a 'Dashboard' through which to manage an entire cloud environment. However, in some cases, a 'Dashboard' may lead to less sophisticated functionality overall. All cloud vendor specific functionality may not be supported through a CMP dashboard and operations staff may have to rely on vendor specific consoles for some capabilities outside of the common 'Dashboard.' Agencies seeking to fully leverage cloud-native functionality may consider using CMPs in combination with cloud-native tools for basic overview and functions across an entire environment.

Analysis of Alternatives

Overview

The AoA is a qualitative assessment of multi-cloud and hybrid cloud architectures against a set of six evaluative criteria. First, the criteria will be defined and, then, both the multi-cloud and hybrid cloud architectures will be assessed against them.

The goal of the AoA is to provide a side-by-side comparison of multi-cloud and hybrid cloud architectures to help make agencies aware of the relative benefits and tradeoffs of each. Cloud architectures will not be scored because that would point to a recommendation of one architecture over another, which this guide intends to avoid. A one-size-fits-all solution is not appropriate for the varying IT environments across the federal community.

Evaluative Criteria

Cost Effectiveness concerns the costs associated with cloud architecture, relative to the impacts on effectiveness. For example, in a typical IaaS solution, cost savings may occur through a decreased need for staff dedicated to hardware maintenance, allowing them to focus on application deployments and other value-add projects. However, you should note that, in some cases, cost effectiveness may not translate into lower total cost. Indeed, as your IaaS provider creates more virtual servers to meet demand, costs will increase. The extent that costs do increase will depend, in part, on how well the operation of each cloud is optimized.

Manageability is the ease by which a given cloud architecture can be monitored, maintained, and controlled by operations staff. By having appropriate cloud orchestration tools and governance in place, an agency is well-equipped to handle the increasing complexity of managing multiple cloud services. Manageability also means interoperability and standardization, wherein one product or system within a cloud environment can work with another because they adhere to the same technical standards. The downstream effect is that operations staff are relieved of tedious, repetitive, and time-consuming tasks.

Performance is the speed by which a cloud service or cloud-based application operates. A central part of performance in cloud computing is scalability, or the ability of a service or application to handle a sudden increase in demand. In particular, scaling of the network, storage, and compute resources, also known as vertical scaling, generally increases performance. If your agency experiences large fluctuations in the number of end users, for example, it should weigh performance and scalability as important considerations.

Reliability is the ability of a cloud service or cloud-based application to function as needed by users. IT staff should reasonably expect that an application or service is available on demand, is secure, and offers the functionality necessary to complete the tasks at hand.

Because completely continuous operation is not realistic, a critical consideration for your agency is the impact of downtime on mission-critical functions supported by its IaaS solution, and how a given architecture may help mitigate that impact.

Security and Privacy refer to the safeguards used to prevent unauthorized access to cloud-based applications, infrastructure, and data. An IaaS environment may be a target for cyberattacks if the CSP misconfigures authentication or security standards, or if attackers can break authentication and encryption. Under this criterion, one cloud architecture is considered favorable over another if it is better able to protect sensitive data and reduce the attack surface.

Workforce Requirements refer to new knowledge and skills needed by employees to implement and manage a multi-cloud or hybrid cloud environment effectively. Though costly, training often plays a critical role in providing employees with the requisite knowledge and skills. Thus, workforce requirements are favorable for an agency when they are low, not high, because the workforce is able to adapt effectively to the new cloud environment using the knowledge and skills they already have.

Cloud Architecture Alternatives Matrix

Table 8 is an alternatives matrix that describes the extent to which multi-cloud and hybrid cloud architectures satisfy the evaluative criteria: manageability, workforce requirements, cost effectiveness, security and privacy, reliability, and performance.

Table 8. *Cloud architecture alternatives matrix.*

Criteria	Multi-Cloud	Hybrid Cloud
Cost Effectiveness	Multi-cloud architecture can scale entirely according to demand and, thus, agencies only pay for resources when there is demand. CMPs can help to apply cost optimization techniques (i.e., attaining the lowest rates over several clouds) and reduce financial inefficiencies associated with wasteful processes.	Agencies can keep legacy applications on-premises and avoid the often-costly process of migrating them to the cloud. However, this benefit may not offset the considerable costs associated with workforce upskilling and on-premises server hardware, software licenses, and maintenance.
Manageability	CMPs offer streamlined management of multi-cloud architecture, with control of public and private clouds well, if not fully, integrated into a single interface.	Even with recent improvements in CMPs, management of on-premises infrastructure in tandem with IaaS can still pose interoperability and standardization challenges.
Performance	Multi-cloud architecture can leverage horizontal and vertical scaling from public CSPs, and can offer high availability for production applications.[14] At the same time, it avoids the latency bottlenecks that can arise from on-premises infrastructure.	Hybrid cloud architecture can suffer from latency issues when there is a performance mismatch between on-premises infrastructure, private cloud, and public cloud. To leverage the performance benefits of cloud, agencies need to carefully consider how data and metadata are handled in an IaaS solution.

[14] Scaling can be horizontal or vertical. Horizontal scaling is the addition of an identical series of virtual machines to an existing pool of computing resources. Vertical scaling is the addition of a higher series of virtual machines to an existing pool of computing resources.

Table 8, Continued. *Cloud architecture alternatives matrix.*

Criteria	Multi-Cloud	Hybrid Cloud
Reliability	Multi-cloud architecture offers a high degree of reliability, especially in the case of redundant multi-cloud architecture as a failover strategy. Redundant multi-cloud architecture can support mission-critical applications that cannot experience downtime, and meet high user demand through horizontal and vertical scaling.	Generally, an on-premises data center would require substantial resource investments in building and maintenance to match the reliability of a public CSP. On-premises infrastructure, therefore, may increase the risk of service outages, though this risk may be mitigated by redundant hybrid cloud architecture.
Security and Privacy	Multi-cloud security infrastructure is typically easier to manage, cheaper, provides many features, and is shared with best-in-class CSPs. API-based security services rapidly extend new/additional capabilities (e.g., Zero Trust Network Access) throughout an agency's cloud, often at zero additional cost.[15] Importantly, as the Federal Government shifts to zero trust, cloud-native zero trust solutions can be readily integrated into multi-cloud architecture.[16] Thus, a multi-cloud environment which adopts zero trust significantly reduces the attack surface.	Hybrid cloud requires a decentralized approach to enterprise security. This generally means additional applications, monitoring, time-to-value, and cost. New security features in hybrid cloud environments require extensive testing to ensure predictable behavior, as each dependency may react differently. Many new security features (e.g., Zero Trust Networking Access and Single Sign-On) present significant problems when applied to legacy applications and infrastructure, complicating risk management.
Workforce Requirements	Increased hiring and training efforts, including those to integrate silos, are necessary for the IT workforce to become proficient with multiple tools, providers, and systems.	There is a limited workforce with the requisite skills to handle the greater complexity of hybrid cloud architecture, and expansion of it through cross-silo employee initiatives is both costly and time-consuming.

[15] Zero Trust Network Access refers to the capability of security products and services to authenticate the identity and context of users.
[16] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

Determine Your IaaS Cloud Solution

As your agency considers multi-cloud and hybrid cloud architecture, use **Table 9** to determine which IaaS cloud solution may be more appropriate. It displays key considerations, provides corresponding recommendations, and maps them to the evaluative criteria discussed in the Analysis of Alternatives section. It is not intended to be exhaustive, and your agency very likely will arrive at additional considerations to inform the decision on which cloud architecture to move towards (if at all).

Table 9. *List of considerations for multi-cloud and hybrid cloud architecture.*

#	Criteria	Consideration	Recommendation
1	Cost Effectiveness Workforce Requirements	Is your agency seeking to reduce labor costs associated with hardware maintenance?	Entirely on the cloud, **multi-cloud** frees up staff from many hardware-related tasks and is therefore recommended.
2	Cost Effectiveness Workforce Requirements	Is your agency seeking to reduce labor costs associated with on-premises back-up and restore solutions?	Again, **multi-cloud** frees up staff from many hardware-related tasks and is therefore recommended.
3	Manageability	Does your agency require on-premises servers, storage, and networking?	If your agency seeks to retain on-premises servers, storage, and networking, then **hybrid cloud** is recommended.
4	Manageability	Is your agency running on-premises Infrastructure as Code (IaC)?	If your agency runs IaC, then **hybrid cloud** can utilize on-premises and cloud IaC programs such as Terraform and Jenkins.

Table 9, Continued. *List of considerations for multi-cloud and hybrid cloud architecture.*

#	Criteria	Consideration	Recommendation
5	Manageability	Do you have on-premises and cloud endpoints that are managed and/or monitored with specific applications?	If your agency seeks to manage and/or monitor applications across on-premises and multi-cloud environments, then **hybrid cloud** is the recommended approach.
6	Manageability	Does your agency's on-premises application connect to other on-premises devices that are not cloud-suitable?	If your agency's on-premises application connects to other on-premises devices that are not cloud-suitable, then **hybrid cloud** is recommended. Hybrid cloud can utilize on-premises connectivity of these applications and connected devices, and still take advantage of existing CSP environments as described in #11.
7	Manageability	Does your agency's on-premises application run on a legacy operating system that is not supported on the cloud?	If your agency seeks to retain an on-premises application that is not supported on the cloud, then **hybrid cloud** is recommended. Hybrid cloud can utilize on-premises dependencies of legacy applications and still take advantage of existing CSP environments as described in #11.
8	Manageability	If feasible, does your agency seek to migrate its on-premises infrastructure to the cloud?	If your agency wants to eliminate all or part of the on-premises footprint, then **multi-cloud** is recommended. Discovery and assessment of cloud readiness for migration to public and/or private cloud would be required for all applications.

Table 9, Continued. *List of considerations for multi-cloud and hybrid cloud architecture.*

#	Criteria	Consideration	Recommendation
9	Manageability Security and Privacy	Is your agency's on-premises application not approved for the cloud or is software not cloud-ready?	Some applications may not be cloud-approved by an agency or governing body. If your agency's on-premises application is not approved for the cloud or the software is not cloud-ready, then **hybrid cloud** is recommended. Hybrid cloud can utilize on-premises dependencies of these applications and still take advantage of existing CSP environments as described in #11.
10	Manageability Reliability	Do you need to alleviate a dependency on one CSP?	If your agency does not have on-premises infrastructure and wants to leverage best-of-market capabilities or mitigate vendor lock-in, then **multi-cloud** is the recommended approach.
11	Performance	Does your agency have on-premises applications that require low latency?	**Hybrid cloud** is recommended if your agency's applications require low latency and still connect to other applications and CSPs. Through an extended VPC or virtual network (VNET) on-premises, low latency applications can stay on-premises and continue to be part of an extended CSP environment.
12	Performance	Should your agency's entire IT infrastructure be scalable?	If your agency seeks an IT infrastructure which scales entirely according to demand, then **multi-cloud** is recommended.

Table 9, Continued. *List of considerations for multi-cloud and hybrid cloud architecture.*

#	Criteria	Consideration	Recommendation
13	Security and Privacy	Is your agency's data protected by the Health Insurance Portability and Accountability Act (HIPAA)?	Either **multi-cloud** or **hybrid cloud** may be an effective approach to handle HIPAA-protected data. If your agency is using a CSP that does not comply with HIPAA, then **hybrid cloud** is recommended. However, an increasing number of CSPs now offer agencies sufficient security, particularly with additional security controls layered on top of what CSPs inherit from the Federal Risk and Authorization Management Program (FedRAMP).
14	Security and Privacy	Will your agency store sensitive applications and data on a private cloud?	With appropriate Authorization to Operate (ATO) and security controls and protocols, a private cloud may be a suitable host for sensitive applications and data. **Multi-cloud** is recommended if your agency seeks to store sensitive applications and data on a private cloud with these controls and protocols. Furthermore, as more CSPs become FISMA High compliant, keeping data on-premises offers little to no additional protection.
15	Workforce Requirements	Is your agency's on-premises application managed by application/system owners who are resistant to moving their application to the cloud?	If your agency's application/system owners are resistant to moving their application to the cloud, then **hybrid cloud** is recommended. Hybrid cloud architecture can utilize on-premises applications that face resistance to the cloud and still take advantage of existing CSP environments as described in #11.

Conclusion

Your agency's decision to use multi-cloud or hybrid cloud is an instrumental part of its larger IT strategy. This guide contains a variety of resources to help your agency determine which cloud architecture—multi-cloud or hybrid cloud—may be appropriate for its IT modernization efforts. The use cases, SWOT analyses, management best practices and recommended management shifts, analysis of alternatives, and architecture checklist are all valuable tools to help your agency make that decision with confidence.

For more information, please contact the Data Center and Cloud Optimization Initiative (DCCIO) Project Management Office (PMO) at dccoi@gsa.gov.

Appendix 1: Emerging Technologies

Edge Computing

Edge computing places time-sensitive data processing in close geographical proximity to the "edge," or the source of the data. Critically, only processed data, not all raw data, is sent to a wide area network or the cloud for storage and distribution. Driven by recent advances such as the Internet of Things (IoT) and 5G, edge computing allows for significantly faster processing and data analysis compared to a centrally managed approach via data centers or the cloud. Thus, through edge computing, the performance of applications with real-time computing power, like those on IoT devices, is not hindered by latency issues. Further, adopters of edge computing may also experience lower network costs because the flow of data over the network decreases when processed data resides at the edge.

Distributed Cloud

A **distributed cloud** refers to a public cloud distributed to different geographic locations, while public CSPs retain control over the operations, governance, and security and privacy. By incorporating edge computing, distributed cloud contrasts with previous definitions of cloud, which do not include location. These locations at the edge, or "substations," allow for economies of scale: public CSPs may share installation and operating costs associated with a "substation," sufficiently lowering prices to attract customers who seek improved performance, reliability, and compliance.[17] Importantly, distributed cloud solutions can go beyond IoT and 5G to a range of other location-dependent use cases. For example, public CSP control of on-premises data centers and community cloud solutions for densely populated regions.

[17] Plummer, D., Smith, D., Anderson, E., & Cearley, D. (2020, April 24). '*Distributed Cloud' Fixes What 'Hybrid Cloud' Breaks*. Gartner. https://www.gartner.com/document/3984151

Appendix 2: Additional Resources

- Application Lifecycle Framework
- Application Lifecycle Framework Templates
- The Application Rationalization Playbook
- Cloud Strategy Guide*
- Cloud Strategy Artifacts*
- Evaluation of Cloud Computing Services Based on NIST SP 800-145
- Guiding Principles of Edge Computing*
- Small and Micro Agency Cloud-Strategy Toolkit*

Resources noted with an asterisk require an account with Max.gov.

Appendix 3: List of Acronyms

Abbreviation	Meaning
API	Application Programming Interface
ATO	Authorization to Operate
CMP	Cloud Management Platform
CMS	Cloud Management Service
CSP	Cloud Service Provider
DCCOI	Data Center and Cloud Optimization Initiative
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act of 2002
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IoT	Internet of Things
IT	Information Technology
PaaS	Platform as a Service
PMO	Program Management Office
SaaS	Software as a Service
SWOT	Strengths, Weaknesses, Opportunities, Threats
TCO	Total Cost of Ownership
TIC	Trusted Internet Connection
VNET	Virtual Network
VPC	Virtual Private Cloud