

Memorandum

Software Technology

August 8, 2022

To: Members of the Board
From: Josh R. Williams, Senior Analyst
Thru: Monica R. Valentine, Executive Director
Subject: **Software Technology Guidance Updates** (Topic E)

INTRODUCTION

At the April 2022 meeting, the Board agreed with staff's proposed cloud-service arrangement characteristics and asset-guidance framework. Members observed that it is particularly important to continue to research and deliberate whether cloud-service arrangements can meet the essential characteristics of an asset from SFFAC 5, *Definitions of Elements and Basic Recognition Criteria for Accrual-Basis Financial Statements*.

The attached issues paper provides an analysis on (1) whether different types of cloud-service arrangements can meet the essential characteristics of an asset and (2) the user benefits and preparer challenges with reporting cloud-service arrangements as assets. For this session, staff is only requesting the Board's feedback on the issues paper proposals. Staff is not requesting the Board to make an official decision at this time on whether cloud service arrangements are assets for financial reporting purposes.

REQUEST FOR FEEDBACK BY August 19, 2022

Prior to the Board's August meeting, please review the attached staff recommendations and analyses and respond to the questions by August 19, 2022.

Please submit responses to Josh Williams at WilliamsJR@fasab.gov with a cc to Monica Valentine at ValentineM@fasab.gov.

NEXT STEPS

Pending Board feedback, staff plans to continue to engage with the working group and some cloud-service providers to further explore the proposed asset possibilities for cloud-service arrangements from this issues paper. Staff will then present different asset reporting options to the Board along with further analysis of the costs and benefits of reporting guidance.

ATTACHMENTS

1. Staff Recommendations and Analyses
2. FASAB Software Technology Definitions
3. Asset Guidance Framework
4. Intangible Assets Project Plan

Staff Analysis

Software Technology

August 8, 2022

CONTEXT

Background

At the February 2022 meeting, staff presented an issues paper that provided a framework for developing reporting guidance updates for software technology assets. Specifically, the issues paper recommended a scope and project plan for developing updates for software guidance based on specific needs identified during research. The scope consists of four major categories of software resources that staff plans to address individually in the following order:

1. Cloud-service arrangements
2. Shared services
3. Internal use software updates
4. Other software technology

Staff is currently focusing on reporting-guidance needs for cloud-service arrangements. Research indicated that federal entities are using cloud services at an increasing rate for operational purposes similar to internally developed software, generally due to the need for less investment risk and more flexibility to alter the amount and type of services received based on current needs. Therefore, it is critical to address reporting guidance for this commonly used software-technology resource to ensure reporting consistency throughout the federal government.

At the April 2022 meeting, staff presented characteristics of cloud-service arrangements along with an asset-guidance framework for which to apply the characteristics. The framework analyzes previous asset-guidance decisions that will assist the Board when deliberating whether cloud-service arrangements can represent assets in the federal government¹. There were three primary takeaways from the discussion:

- The National Institute of Standards and Technology's (NIST) cloud-computing characteristics are widely accepted and used in the federal government.
- Based on the asset-guidance framework, it is appropriate to approach cloud-service arrangements as lease-type transactions that provide a federal entity

¹ See Attachment 3 for Asset Reporting Guidance Framework illustration.

access to a provider's software technology resources for the federal entity to use as internal use software for a specified period.

- More research and outreach is needed to develop an informed decision on whether cloud-service arrangements can meet all of the essential characteristics of an asset established in SFFAC 5, *Definitions of Elements and Basic Recognition Criteria for Accrual-Basis Financial Statements*.

The Board supported using the NIST's cloud-computing characteristics for developing financial reporting guidance for cloud-service arrangements. Several members agreed with staff's observation that federal entities widely use the NIST cloud-computing characteristics and that it is practical to defer to the information technology (IT) professionals when describing cloud-service arrangements.

The Board agreed with staff's proposed asset-guidance framework and observation that it is particularly important to continue to research and deliberate whether cloud-service arrangements can meet the essential characteristics of an asset from SFFAC 5. Some members noted that for an asset to exist, the cloud-service arrangement must represent economic benefits and services that the federal government can use in the future. Other members stated that it is critical to determine whether a consumer of a cloud service could control access to the economic benefits and service of the underlying resource and, particularly, if the user could deny or regulate access to others in accordance with the arrangement.

At the June 2022 meeting, two panelists from the General Services Administration (GSA) provided the Board an educational session on cloud-service arrangements. The panelists provided members an overview of the characteristics, service models, and deployment models of cloud computing and discussed ways that federal entities procure and pay for cloud services. Additionally, Board members, staff, and panelists discussed potential financial reporting needs and challenges associated with cloud-service arrangements.

Research

Staff continued to conduct research and engage with the working group to provide the Board with relevant information so that members can ultimately make an informed decision on whether cloud-service arrangements represent assets for financial reporting purposes. Staff specifically focused on learning the different ways federal entities procure and pay for cloud services in order to assess whether they could meet the SFFAC essential characteristics of an asset.

Staff continued to research the NIST Cloud Computing publication² for a deeper dive on the characteristics and models of cloud computing. Additionally, staff referred to GASB

² National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145, September 2011

Statement No. 96 for insight into how an existing standard considers the different modes of cloud service arrangements in the scope of reporting guidance.

Staff analyzed multiple cloud service schedules from the GSA eLibrary³ website. These schedules offered insight into the ways private vendors offer cloud services to the federal government. Additionally, some working group members provided examples of service schedules that their federal entities use. Staff also held round table discussions with different federal entities to understand how they procure and pay for cloud services.

Staff hosted a working group meeting in July 2022 to discuss the majority of the material in this issues paper. Specifically, the working group discussed:

- The scope of cloud computing characteristics, service models, and deployment models applicable in the federal environment
- How software licenses apply to cloud services
- Major categories of cloud-service arrangements in the federal government
- Whether the major cloud-service arrangement categories could meet the essential characteristics of an asset
- Financial reporting benefits and challenges with cloud-service arrangements

Additionally, staff met with a staff member from the Governmental Accounting Standards Board (GASB) to gather insights and lessons learned from GASB Statement No. 96, *Subscription-Based Information Technology Arrangements*. The staff members specifically discussed scope possibilities and potential issues with cloud-service arrangement guidance.

This analysis includes working group member comments from the meeting and round table discussions so that the Board is aware of the working group's thoughts and concerns about staff's proposals.

RECOMMENDATIONS AND ANALYSES

This topic is a continuation from the April 2022 meeting discussions and June 2022 educational session. Specifically, this issues paper proposes the following:

- A framework of cloud-service arrangements that could meet the essential characteristics of an asset for financial reporting purposes
- Potential benefits and challenges of reporting cloud service arrangements as assets in federal financial reports

³ GSA eLibrary provides a source for the latest GSA contract award information - <https://www.gsaelibrary.gsa.gov/ElibMain/home.do>

Staff intends for the proposals in this issues paper to illicit further discussion and feedback from the Board so that staff can continue to fine-tune a scope and framework for cloud-service arrangement reporting guidance. Staff is not asking the Board to make any official decisions on cloud-service arrangements at this time.

RECOMMENDATION

CLOUD-SERVICE ARRANGEMENT ASSET REPORTING FRAMEWORK

During the April 2022 meeting, members agreed with staff that it is particularly important to continue to research and deliberate whether cloud-service arrangements can meet the essential characteristics of an asset from SFFAC 5. Staff determined it necessary to analyze the essential characteristics of an asset with specific types of cloud-service arrangements that exist among federal entities rather than from a broad, general perspective. Therefore, this analysis focuses on whether the different cloud-service models, deployment models, and arrangement categories could meet the essential characteristics of an asset. Staff requests that members provide feedback on the asset reporting proposals in the following analysis.

ANALYSIS

NIST cloud computing definition, characteristics, and models

During the April 2022 meeting, the Board supported using NIST’s cloud-computing characteristics for developing financial reporting guidance for cloud-service arrangements. Several members agreed with staff that federal entities widely accept and use the NIST cloud-computing characteristics and that it is practical to defer to the IT professionals when describing cloud-service arrangements.

During the June 2022 educational session, the GSA speaker referred to the NIST cloud-computing characteristics to describe cloud services in the federal government. The speaker also referred to the NIST when explaining different service and deployment models of cloud services that this analysis will address in detail.

Upon further research, staff noticed that in almost all of the GSA eLibrary schedules, the cloud-service provider references the NIST cloud-computing characteristics to describe the services that they offer. In fact, the vendors often state in the schedule that their services meet the NIST cloud-computing characteristics in order for their services to be classified in the Special Item Number (SIC) 518210C, *Cloud Computing Services*. However, this does not mean that all cloud-service arrangements in the federal government strictly meet the NIST characteristics.

Staff is confident that the NIST cloud-computing characteristics are used extensively throughout the federal government. Therefore, staff believes that the framework for future reporting guidance on cloud-service arrangements should predominantly refer to

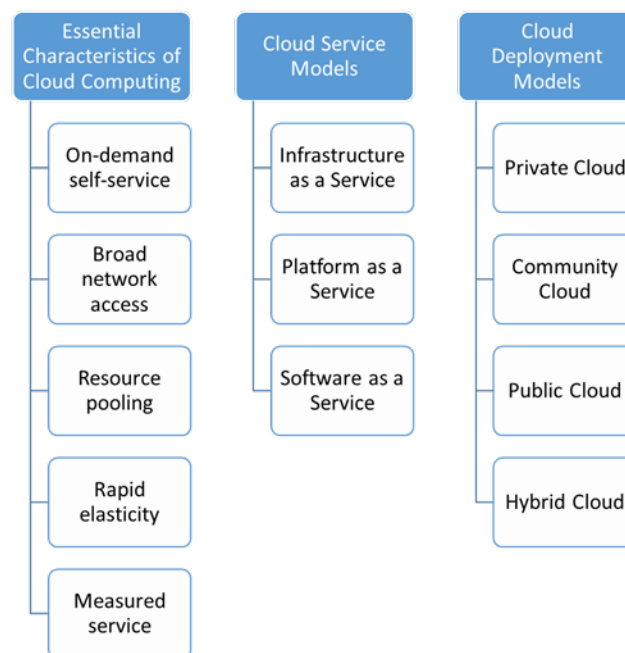
the NIST cloud-computing definition, characteristics, service models, and deployment models. The following paragraphs provide excerpts from the NIST special publication.

The NIST definition of cloud computing is 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.

The NIST considers cloud computing to consist of five essential characteristics, three service models, and four deployment models as depicted in the chart below.

NIST Cloud Computing Characteristics and Models



NIST explains the five essential characteristics of cloud computing as follows:

- ***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.

The NIST explains the three service models of cloud computing as follows:

- *Software as a Service (SaaS)* - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure⁴. 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.
- *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.
- *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).

⁴ NIST explains that a cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing.

A report by the Congressional Research Office⁵ provides a useful analogy to understand the different service models:

- A simple local-computing analogy for these three kinds of services would be the purchase of a desktop computer, which serves as infrastructure on which the user installs a chosen operating system such as Windows or Linux and uses it as a platform to create custom applications and run whatever software is needed. By providing these infrastructure, platform, and software services remotely, a cloud provider frees its customers from having to provide local infrastructure and support. In the case of IaaS, the user need not have a local workstation, using instead a thin client with minimal need for computing power.

During the June 2022 meeting, the GSA presenter explained the three cloud-service models by using pizza service as an analogy. He explained how there are different levels of cloud-service provider and customer responsibilities depending on the cloud model. For example, physical servers installed on-site, like a homemade pizza, are not considered cloud and are completely the customer's responsibilities. Like a take and bake pizza, with IaaS the cloud-service provider has some management responsibilities, such as managing the data center and network infrastructure while the customer manages everything else. Similar to a pizza delivery service, with PaaS, the cloud service provider has more management responsibilities, such as managing operating systems and implementing security patches while the customer still manages everything else, such as software applications, data, and account access. Like dining in at the pizza shop, with SaaS, the cloud service provider has even more management responsibilities, such as managing network security controls and software applications. The presenter caveated that no matter the cloud model, the customer always manages their data and account rights.

The NIST explains the three deployment models of cloud computing as follows:

- *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

⁵ Congressional Research Service, *Cloud Computing: Background, Status of Adoption by Federal Agencies, and Congressional Action*, R46119, March 25, 2020

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).

Staff believes it is important for the Board to review and understand cloud-computing and related terms in the federal environment without expanding upon or clarifying the NIST guidance. It is important to expand and clarify cloud-related terms only for financial reporting reasons and to otherwise leave the IT guidance to the IT professionals. For example, it would be appropriate for future guidance to explain the data security implications of private versus public cloud only if there were an accounting or financial reporting reason for doing so.

Staff is not suggesting that reporting guidance for cloud-service arrangements should scope out cloud services that do not strictly apply to the NIST cloud computing characteristics and models. It will be important to develop a flexible reporting guidance scope so that preparers can make judgements on whether any given cloud-service arrangement applies to the guidance. However, staff believes that the Board should use the NIST report to understand the aspects of cloud services in the federal government for which to develop an asset-reporting framework.

Cloud-service arrangement categories

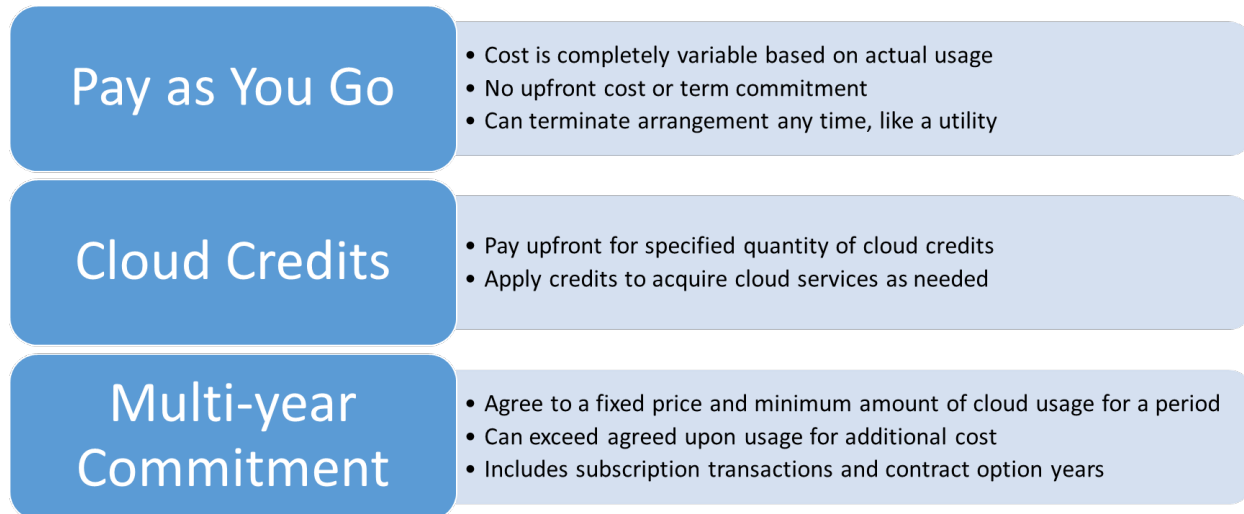
Staff's current working definition for cloud-service arrangement is:

- A cloud-service arrangement is a contract or agreement that provides a federal entity the right to access and use information technology resources provided by a vendor over the internet without the federal entity taking possession of the information technology resource on its own hardware or systems.

Since the April 2022 meeting, staff has devoted a significant amount of time in researching the different ways that federal entities procure and pay for cloud services. As stated previously, staff analyzed multiple cloud-service schedules from the GSA eLibrary and held round table discussions with different federal entities to discuss examples of cloud-service arrangements. Based on this research, staff developed three primary categories of cloud-service arrangements used throughout the federal government. The following chart depicts and summarizes the categories.

(Chart on next page)

Cloud-service arrangement categories



With the pay-as-you-go category, federal entities pay a cloud-service provider in arrears for actual usage based on established measurement criteria. Additionally, there is no upfront payment, usage, or term commitment. The federal entity can start and stop service when desired. These types of arrangements especially meet all five NIST cloud-computing characteristics and most resemble a utility arrangement. It appears that GSA schedules encourage this type of cloud arrangement.

With cloud credits, federal entities pay upfront for a specific quantity of cloud credits that they can then apply to receive various cloud services on demand. This category is similar to the pay-as-you-go category except that consumers pay for a fixed usage amount upfront rather than paying for variable usage in arrears.

With multi-year commitment arrangements, federal entities commit to purchase a minimum amount of cloud services at a fixed price from a vendor for a specified period. However, the federal entity may be able to exceed the agreed upon usage for an additional cost. Federal entities often enter into this type of arrangement to secure a discounted price in exchange for a usage commitment. This type of arrangement can consist of fixed subscription type payments and contract option years.

Staff did not receive comments from working group members that indicated a need to create another category and received general agreement that the three proposed categories largely capture the primary types of cloud-service arrangements in the federal environment. A few IT personnel have mentioned the term “reserved instance” to describe a type of cloud-service arrangement. However, staff currently understands reserved-instance arrangements as synonymous with the multi-year commitments category described above.

One working group member confirmed that multi-year commitment type arrangements typically involved the consumer committing to a minimum dollar amount of cloud services over a set period. They described the arrangement as a minimum guarantee.

Another working group member confirmed that for a cloud credit arrangement, their agency actually pays upfront and compared the arrangement to purchasing a phone card. However, others have mentioned that they do not actually pay upfront due to appropriation limitations. One working group member stated that cloud credits could span multiple years with their federal entity.

One working group member questioned if pay-as-you-go arrangements still involved some type of term-based agreement between the vendor and federal entity and if it were difficult for a federal entity to quickly stop and start cloud services due to implementation and security requirements. Another working group member replied that various requirements could make it challenging and rigid for a federal entity to start and stop service quickly. However, cloud-service providers are typically happy to sell cloud services by the minute without any long-term expectations.

Staff is confident that the three cloud-service arrangements categories described in this analysis largely covers the ways that federal entities procure and pay for cloud services. However, it is possible that there are other types of cloud-service arrangements not captured by the three categories or that blend into multiple categories. Staff will continue to be on the lookout for other types of cloud-service arrangements in the federal environment.

Cloud-service arrangement asset analysis

During the April 2022 meeting, staff provided thoughts on whether cloud-service arrangements could meet all of the essential characteristics of an asset established in SFFAC 5. Paragraph 18 of SFFAC 5 states, “An asset is a resource that embodies economic benefits or services that the federal government controls.” Paragraph 22 of SFFAC 5 breaks the definition down to the essential asset characteristics. The concepts state that to be an asset of the federal government, a resource needs to possess the following two characteristics:

- The resource embodies economic benefits or services that can be used in the future
- The government controls access to the economic benefits or services and, therefore, can obtain them and deny or regulate the access of other entities

Furthermore, paragraph 31 of SFFAC 5 states that “Possession or ownership of a resource normally entails control of access to the economic benefits or services embodied in it, but that is not always the case. Whereas control of access is an essential characteristic of an asset, possession or ownership is not.” The same paragraph goes on to say that – “through a lease arrangement the government may control access to the economic benefits or services embodied in a resource that it does not own.”

The Board agreed with staff that it is important to continue to research and deliberate whether cloud-service arrangements could meet the essential characteristics of an

asset. Some members emphasized that for an asset to exist, the cloud-service arrangement must represent economic benefits and services that the federal government **can use in the future**. Other members stated that it is critical to determine whether a consumer of a cloud service could control access to the economic benefits or service of the underlying resource and, particularly, if the user could deny or regulate access to others in accordance with the arrangement.

After identifying the previously discussed cloud-service arrangement categories, staff analyzed whether each category could meet the SFFAC 5 essential characteristics of an asset. Additionally, staff considered to what extent the NIST cloud service models (e.g. IaaS, PaaS, and SaaS) and deployment models (e.g. private cloud, public cloud, community cloud, and hybrid cloud) could factor into that determination.

Essential characteristics of an asset - control

Staff believes that all three cloud-service arrangement categories largely meet the “control” characteristic of an asset. As long as the federal entity has entered into a contract or agreement to pay a cloud-service provider for access to cloud-based IT resources, the federal entity would generally have control over the economic benefits and services of that resource and could regulate access to the IT resource in accordance with the contract or agreement. Cloud-service arrangements do not appear to provide the level of control that possession or ownership of software licenses⁶ and internally developed software provides. However, per SFFAC 5, paragraph 31, ownership and possession are not necessary to meet the control criteria.

The NIST discusses various levels of consumer control across the cloud-service models. However, “control” is a term of art in SFFAC 5 with a very specific meaning as discussed above. During the June 2022 educational briefing, GSA mentioned that no matter the cloud-service model, the federal entity always manages their data and account rights. In other words, even if the federal entity has more management responsibilities or control over the IT resources for IaaS versus SaaS, staff believes that all three service models meet the SFFAC 5 control criteria. It appears that no matter the service model, the federal entity would have the ability to control access to the economic benefits or services of that cloud-based resource and could obtain them and deny or regulate the access of other entities per the terms of the contract or agreement.

⁶ After discussions with the working group, staff considers the term “license” to have different meanings depending on the context.

Software licenses typically describe a software product that gives the consumer various intellectual property rights over a vendor’s underlying software resource. The acquired license in this scenario generally allows the consumer to possess the underlying software resource on their own hardware and/or IT systems.

Cloud licenses typically describe a cloud service that gives the consumer the right to access and use a vendor’s IT resource over the internet without actually possessing the resource on their own hardware or IT systems.

There is not complete agreement on how federal entities use these terms. For example, one working group member cautioned that the term cloud license could be confusing because while it could represent user access to a cloud service, in some situations a consumer could also procure a software license as part of a cloud-service arrangement or that a software license could be included in the cost of a cloud-service arrangement.

Regarding the NIST cloud deployment models, private cloud models would provide a federal entity more exclusive access to the entire underlying cloud resource than would public clouds. However, public cloud is not public space and even with public cloud, the federal entity would be able to deny or regulate access to their cloud service rights in accordance with the arrangement with the provider. Federal entities often do this through passwords and/or access identification security controls.

Additionally, staff does not think it is necessary for a federal entity to have exclusive control over the entire IT resource to consider it an asset. For example, a federal entity may rent a few office rooms in a large office building. That federal entity does not have to own or control access to the entire building to consider its rented rooms as lease assets. Another example is a consumer having access to any generic office in a building full of the same offices. The consumer would not care which office they have rights to but know they have rights to access and use an office building and know that they can exercise that right over others who have not entered into such an arrangement.

Furthermore, staff believes it would not be practical for preparers to analyze individual cloud-service arrangements to determine whether a specific arrangement satisfied the SFFAC 5 control characteristic of an asset. Determining the level of control of individual arrangements based on a spectrum of different variables would be highly subjective and lead to disagreement among preparers and auditors and lead to inconsistent reporting among federal entities. For example, SaaS models often include PaaS and IaaS elements, which would make it difficult for a preparer to reasonably assess a sufficient level of control with the entire arrangement. Therefore, staff believes that the Board should ultimately make an overall determination on whether cloud-service arrangements generally meet the control characteristic of an asset and not leave it up to preparers to assess the level of control for individual arrangements.

One working group member disagreed that all cloud-service arrangements would generally meet the control characteristic of an asset. They suggested that there were a spectrum of different levels of control across the different types of cloud-service models and that some may meet the control characteristic while others may not. For example, a private cloud model would provide a federal entity exclusive control of the IT resource but a public cloud model would not because the federal entity would have no say in who else the public cloud provider provides access. They suggested that the federal entity would be able to deny or regulate access for private clouds but not public clouds. However, the working group member agreed with staff that requiring preparers to assess and judge whether each cloud-service arrangement met the SFFAC 5 control criteria would be extremely burdensome and voiced concern that it would be difficult to implement consistently.

Essential characteristics of an asset – future economic benefits or services

During the April 2022 meeting, some members emphasized the word “future” when stating that for an asset to exist, a resource must represent future economic benefits or services for the federal entity. Therefore, staff analyzed the identified cloud-service

arrangement categories to focus specifically on whether the contract or agreement represents a known economic benefit or service that the federal entity can use in the future.

- *Pay-as-you-go* – This type of arrangement does not appear to represent a future economic benefit or service for the federal entity because neither party to the agreement is obligated to continue meeting their requirements (e.g. timely payment and cloud access) beyond the present. Additionally, the future cash flows are purely variable based on usage and therefore the entity cannot know the future amounts.
- *Cloud credits* – The upfront payment by the federal entity requires the vendor to provide future cloud access to the federal entity. Therefore, the upfront payment transaction would appear to represent a known future economic benefit or service for the federal entity.
- *Multi-year Commitment* – This type of arrangement requires the vendor to provide a minimum amount of future cloud access to the federal entity for a specified price and period so long as the federal entity continues to meet their requirements throughout the period of the agreement (e.g. timely payment). Therefore, the minimum purchase aspect of this agreement would appear to represent a known future economic benefit or service to the federal entity and would represent known fixed future cash flows.

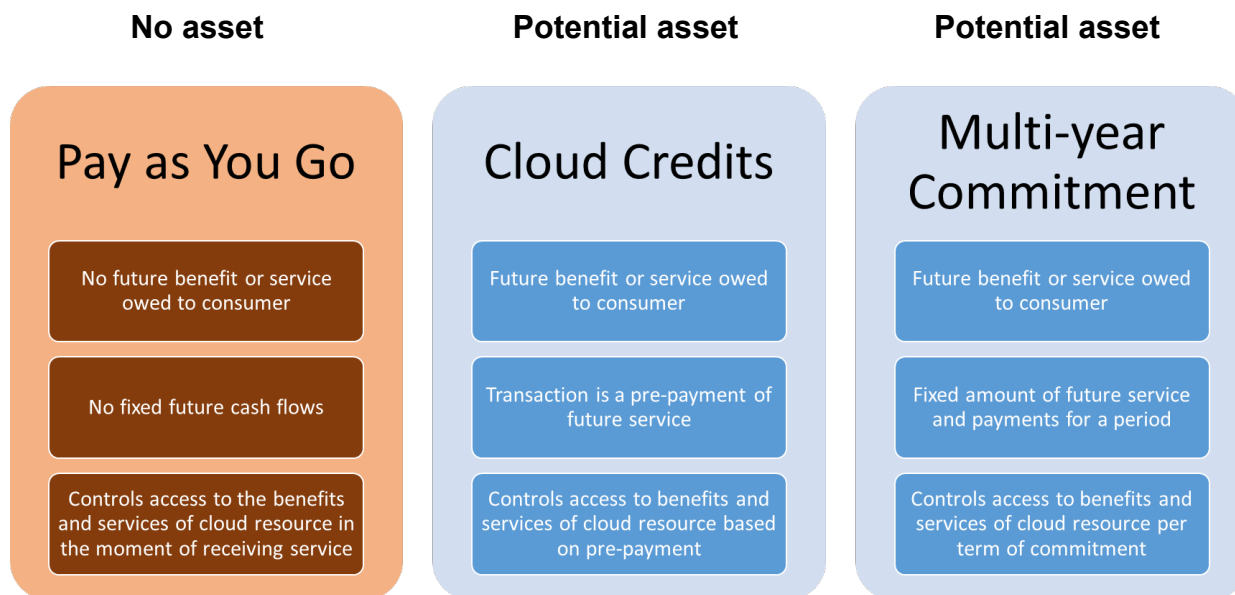
One working group member pointed out that with cloud credit and multi-year commitment arrangements, there may be a future economic benefit or service owed to the federal entity, but it is often not a specific or known economic benefit or service. In other words, the federal entity could apply their cloud credit or minimum purchase agreement to a multitude of cloud services that the provider offers. The working group member suggested that the vagueness of the future service could bring into question whether the cloud-service arrangement meets the essential characteristics of an asset. Staff spoke with another federal entity that indicated that it typically applies cloud credits to a variety of cloud services but that multi-year commitments are typically for a more specific cloud service.

One working group member stated that multi-year commitment cloud-service arrangements include a minimum purchase guarantee but are typically executed pay-as-you-go. Therefore, they questioned if multi-year commitments could result in the federal entity not actually using the minimum purchase amount as that could make it difficult to assess whether there is a known future economic benefit or service for the federal entity. Another working group member replied that the contract or agreement typically holds the federal entity and provider to the payment and service requirements of the multi-year commitments. One federal entity informed staff that cloud service customers are often able to sell back unused cloud usage to a marketplace, which staff believes is indicative of control over a resource. However, it may be difficult for federal entities to do this due to fiscal laws and budgetary mechanisms.

Cloud-service arrangement potential assets

In accordance with the previously discussed analysis, staff developed the following framework of potential cloud-service arrangement assets.

Cloud-service arrangement asset framework



As previously stated, staff believes that any type of cloud-service arrangement would generally meet the control criteria from SFFAC 5. As long as the federal entity has entered into a contract or agreement to pay a cloud-service provider for access to cloud-based IT resources, the federal entity would generally have control over the economic benefits and services of that resource and could regulate access to its rights to use the IT resource in accordance with the contract or agreement. Staff does not believe that the spectrum of control that the different NIST cloud service and deployment models offer are relevant for financial reporting purposes because they all could theoretically meet the definition of control per the SFFAC 5 essential characteristics of an asset. Additionally, determining sufficient level of control for individual cloud-service arrangements would be highly subjective and practically difficult for preparers to implement.

On the other hand, staff believes it is necessary to analyze the different categories of cloud-service arrangements to determine whether the mechanisms of the contract or agreement represent an economic benefit or service that the federal entity could use in the future. Staff believes this would be a more objective decision for preparers as it relies on the payment and service delivery aspects of the agreement.

In summary, staff believes that the pay-as-you-go arrangement does not meet the SFFAC 5 essential characteristics of assets. However, staff believes that both the cloud credit and multi-year commitment types of cloud-service arrangements could potentially meet both SFFAC 5 essential characteristics of assets. Specifically, staff believes there is opportunity to report cloud credit arrangements as a type of pre-paid expense and multi-year commitment arrangements similar to lease assets.

Note that staff is using the phrase “potential asset” when describing cloud credits and multi-year commitments because staff sees potential asset reporting options for these kinds of arrangements, in theory. However, further research is necessary to understand the practicalities and difficulties of preparers actually reporting them as assets. Some working group members have indicated support for staff’s current positions and have indicated that the asset reporting options sound feasible in theory while some other working group members have voiced disagreement or concern with the practicalities of doing so.

Some working group members acknowledged that cloud-service arrangements may meet the SFFAC 5 asset characteristics but stated it was difficult to envision them as capital assets in the general sense as they view them as service contracts. However, some working group members agreed that in theory, federal entities were using cloud services to finance an IT resource from another entity instead of developing it or purchasing it. Staff agrees that reporting cloud-service arrangements as assets would push the boundaries of the current asset guidance framework by essentially considering a service contract as an asset. This could open the door for future questions on whether other types of service contracts are assets.

Nevertheless, staff believes they have narrowed the scope on where there is asset-reporting potential for cloud-service arrangements in the federal government. However, staff recommends more research to properly understand the feasibility of reporting them as assets in financial reports.

Staff is only requesting the Board’s feedback on the recommended asset-reporting framework for cloud-service arrangements. Pending the Board’s feedback, staff will continue to work with the working group and reach out to private cloud providers to gather more information on the categories of cloud-service arrangements that staff has identified in the federal environment. At a future Board meeting, staff plans to provide the Board an issues paper that provides recommendations on a reporting guidance framework for cloud-service arrangements.

Question for the Board:

1. Do members have any feedback on the proposed asset framework for cloud-service arrangements?

RECOMMENDATION

ASSET REPORTING BENEFITS AND CHALLENGES

Concepts from SFFAC 1, *Objectives of Federal Financial Reporting* address four objectives that federal financial reporting should accomplish. Through research and correspondence with the working group, staff developed an analysis of different ways that reporting cloud-service arrangements as assets could contribute to the federal financial reporting objectives. Additionally, staff developed a general list of other potential user benefits and preparer challenges with reporting cloud-service arrangements as assets.

Staff is recommending this list of financial reporting benefits and challenges for members to consider as they continue to deliberate financial reporting guidance needs for cloud-service arrangements. This analysis serves as a starting point for deliberating the benefits versus costs of new reporting requirements for cloud-service arrangements.

ANALYSIS

Objectives of Federal Financial Reporting

Staff consulted SFFAC 1 to develop ways that reporting cloud-service arrangements in financial reports could contribute to FASAB's four objectives of financial reporting: budget integrity, operating performance, stewardship, and systems and controls. Staff also elicited the working group's feedback on the objectives and invited further ideas. The following analysis discusses how reporting cloud-service arrangements as assets could contribute to the financial reporting objectives.

Budget Integrity

Paragraph 13 of SFFAC 1 states:

Federal financial reporting should assist in fulfilling the government's duty to be publicly accountable for monies raised through taxes and other means and for their expenditure in accordance with the appropriations laws that establish the government's budget for a particular fiscal year and related laws and regulations. Federal financial reporting should provide information that helps the reader to determine

- *how budgetary resources have been obtained and used and whether their acquisition and use were in accordance with the legal authorization,*
- *the status of budgetary resources, and*
- *how information on the use of budgetary resources relates to information on the costs of programs operations and whether information on the status of budgetary resources is consistent with other accounting information on assets and liabilities.*

Reporting cloud-service arrangements as assets could help with identifying the associated liabilities that a federal entity will pay in the future for the cloud services. This would help identify budgetary resources needed in the future to pay for cloud services.

Operating Performance

Paragraph 14 of SFFAC 1 states:

Federal financial reporting should assist report users in evaluating the service efforts, costs, and accomplishments of the reporting entity; the manner in which these efforts and accomplishments have been financed; and the management of the entity's assets and liabilities. Federal financial reporting should provide information that helps the reader to determine

- *the costs of providing specific programs and activities and the composition of, and changes in, these costs;*
- *the efforts and accomplishments associated with federal programs and the changes over time and in relation to costs; and*
- *the efficiency and effectiveness of the government's management of its assets and liabilities.*

Reporting cloud-service arrangements as assets could help identify cost efficiencies of a federal entity's IT resources by identifying and categorizing the cost for providing federal programs and services, as well as helping management compare costs of different IT resources used in operations (e.g. internally developed software and software licenses).

Stewardship

Paragraphs 15 and 16 of SFFAC 1 states:

Federal financial reporting should assist report users in assessing the impact on the country of the government's operations and investments for the period and how, as a result, the government's and the nation's financial conditions have changed and may change in the future.

Federal financial reporting should provide information that helps the reader to determine whether

- *the government's financial position improved or deteriorated over the period,*
- *future budgetary resources will likely be sufficient to sustain public services and to meet obligations as they come due, and*
- *government operations have contributed to the nation's current and future well-being.*

Reporting cloud-service arrangements as assets could enable financial reports to better portray the financial position of a federal entity by depicting the status of federal assets and associated liabilities. Additionally, this could help identify trends with how much a federal entity is essentially financing a software related asset from a vendor.

Systems and Controls

Paragraph 17 of SFFAC 1 states:

Federal financial reporting should assist report users in understanding whether financial management systems and internal accounting and administrative controls are adequate to ensure that

- *transactions are executed in accordance with budgetary and financial laws and other requirements, consistent with the purpose authorized, and are recorded in accordance with federal accounting standards;*
- *assets are properly safeguarded to deter fraud, waste, and abuse; and*
- *performance measurement information is adequately supported.*

Reporting cloud-service arrangements as assets encourages good internal controls to account for federal assets and associated liabilities and expenses accurately.

The following chart summarizes how cloud-service arrangement asset reporting could contribute to the financial reporting objectives:

Cloud-service arrangements – financial reporting objectives

Budget Integrity	<ul style="list-style-type: none"> • Identify budgetary resources needed for future payments for cloud service arrangements
Operating Performance	<ul style="list-style-type: none"> • Future obligations of providing federal programs • Comparing costs of IT related assets • Efficiency and economy of operations
Stewardship	<ul style="list-style-type: none"> • Status of assets and liabilities affecting financial position • Trends in financing software resources from other entities
Systems and Control	<ul style="list-style-type: none"> • Reporting federal assets and liabilities helps ensure controls are in place to account for costs accurately

One working group member generally agreed with the financial reporting objective analysis but suggested that they already achieve those objectives through their existing practices of analyzing and managing cloud-service costs for their federal entity. They

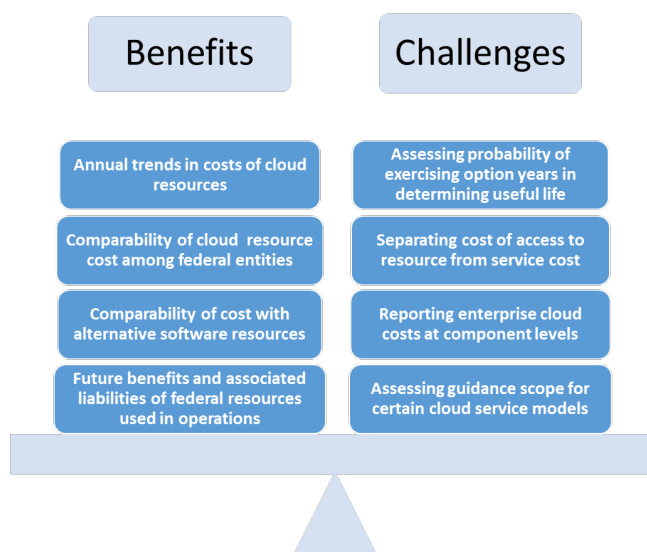
stated that due to other financial management requirements, they already record and analyze cloud-service needs and costs very thoroughly to ensure efficiencies in their federal entity's operations and did not think that additional financial reporting requirements were necessary to encourage that.

One working group member observed that the financial reporting objectives appeared to want predictability with reporting asset value. However, the flexible, on-demand nature of cloud-service arrangements may not easily fit into financial reporting requirements that require predictable future value.

Other reporting benefits and challenges

Staff also considered other user benefits and preparer challenges with reporting cloud-service arrangements as assets. Staff elicited the working group's feedback on the objectives and invited further ideas. The following chart and analysis discusses these potential benefits and challenges:

Financial reporting benefits and challenges



Financial reporting benefits

Reporting cloud-service arrangements as assets in financial reports could help users identify annual trends in cloud service costs at the entity and government-wide levels. Additionally, reporting requirements could help users compare cloud service cost among federal entities and compare cloud service costs with alternative IT operational costs, such as investments in internally developed software or software license subscriptions. It appears federal entities use cloud-service arrangements to finance software assets for internal use that it once may have developed internally. Staff sees similarities to leases that are essentially financing a tangible asset from someone else.

During research, staff found that one federal entity is already performing net present value analysis to compare cloud service cash flows with costs to acquire or develop other internal use software assets. This type of analysis could help federal entities make cost effective decisions on what type of software resources to invest in for operational needs. Finally, reporting requirements could provide transparency on anticipated cash outflows associated with a future economic benefit or service to the federal entity.

One working group member understood the potential reporting benefits but cautioned that overly broad financial reporting without enough context or detail could do more harm than good. They emphasized that every federal entity's mission and operational needs are different and that users could jump to incorrect conclusions without enough detail in the numbers.

Financial reporting challenges

For cloud-service arrangements with multiple option years, it could be difficult for preparers to determine the useful life of an asset due to the difficulty in determining the probability of exercising option years in the future. This is especially true due to the fast changing environment of the IT industry and on-demand and flexible nature of cloud services. One working group member pointed out that often, federal entities procure cloud services only one year at a time due to one-year appropriation limitations, even if the contract presents as a base year with option years. Another working group member stated that their federal entity is not bound by one-year appropriations and therefore enters into cloud-service arrangements with multi-year base terms and option years, such as a base of three years with two-year options. One working group member stated that even with the difficulties, it was still possible to assess a useful life of an arrangement with a cloud service provider and that the benefits outweigh the costs of doing so.

In researching cloud-service arrangement templates, it appeared that the clauses often clearly separated cloud services from professional labor services for implementing and operating cloud services. The contracts typically separated them by special item numbers. However, staff believes some contracts may not clearly separate the two. One working group member pointed out that with cloud services, there are multiple cost components, such as labor, infrastructure, networks, licenses, and code baked into the price of the cloud service, even if the federal entity does not see that level of detail. Staff agrees that it would be difficult for preparers to analyze individual cloud-service arrangements at that level to identify the different types of costs baked into the cloud service price and that with many arrangements it likely would not be possible as the consumer just sees a total price.

One working group member offered that it could be challenging for federal entities to allocate and report enterprise level cloud-service costs at component levels. However, it could also benefit federal reporting entities' cost accounting practices to report enterprise level costs at component levels. In other words, this is both a reporting benefit and challenge.

Several working group members have mentioned a foreseeable challenge with determining whether certain cloud-service models that utilize underlying tangible IT resources (e.g. IaaS) would belong in the lease guidance scope or future cloud-service arrangement scope. For example, what is the difference between leasing a tangible computer server on premise versus an IaaS private cloud service? Most likely a key difference is that there is a service component with a cloud-service arrangement that is not present with a leased server. Leasing a server could be thought of as renting a lawnmower while a cloud-service arrangement is equivalent to paying someone to mow your yard.

In addition, most cloud services consist of a combination of providing access to underlying intangible (e.g. software code) and tangible (e.g. servers and data centers) IT resources. It would be very difficult and burdensome for preparers to have to parse intangible and tangible aspects of the asset for reporting purposes and may even be impossible, as most cloud-service arrangements would not provide that kind of cost detail.

Due to these scope concerns, it is important that future cloud-service arrangement guidance include a very explicit scope that makes it clear to preparers and auditors whether all cloud-service arrangements are intangible or some are leases of tangible property. Staff believes that future guidance should consider any type of cloud-service arrangement, even ones based on underlying tangible IT resources, as intangible software resources because ultimately the cloud-service arrangements serve a software-related purpose in a federal entity's operations. It appears that GASB took this approach with their Statement No 96 scope.

One working group member voiced general concern with the burden of having to report a new asset in financial reports while they are still grappling with other new reporting requirements the Board has issued recently. Another working group member stated that federal entities are already required to deal with several other financial management requirements with cloud services and cautioned that it was important not to issue overlapping requirements without any added benefit. They suggested referring to the Technology Business Model standards for insight when developing reporting guidance. Staff will look into this further.

Staff is only requesting the Board's initial thoughts and feedback on the potential user benefits and preparer challenges of reporting cloud-service arrangements in federal financial reports. Pending the Board's feedback, staff will continue to research and correspond with financial report stakeholders to consider further the costs versus benefits of new reporting guidance for cloud-service arrangements. Staff believes it is important to continue discussing the costs and benefits of reporting guidance ideas throughout the project.

Question for the Board:

2. Do members have any feedback on the potential benefits and challenges of reporting cloud-service arrangements as assets?

Final thoughts and next steps

There are two primary takeaways from this issues paper:

- The potential asset options with cloud-service arrangements
- Reporting benefits, challenges, and contributions to the financial reporting objectives

Since the April 2022 meeting, staff has uncovered different ways that federal entities acquire and pay for cloud services. Because of this, staff has been able to narrow the scope of potential asset options for cloud-service arrangements for the Board to consider. However, staff recommends more research to fully comprehend the reporting possibilities, costs, and benefits. In this issues paper, staff provided their recommendations of whether cloud-service arrangements could meet the SFFAC 5 essential characteristics of an asset based on research, working group correspondence, and their own assessments. However, as staff has pointed out, there are both agreements and disagreements/concerns with staff's assessments among the working group. Staff encourages the Board to offer their thoughts on staff's observations in order to guide future reporting guidance recommendations.

For the next steps, staff plans to continue to engage with the working group and some cloud-service providers to further explore the possibilities of reporting cloud credit and multi-year commitment cloud-service arrangements as assets. Staff will then present different reporting options to the Board along with further analysis of the costs and benefits of reporting guidance.

Disclaimer: This material is presented for discussion purposes only; it is not intended to reflect authoritative views of the FASAB or its staff. Official positions of the FASAB are determined only after extensive due process and deliberations.

Software Technology Definitions

Agile development – an umbrella term used to describe software development methods that incrementally deliver working segments of a product in short iterative cycles instead of delivering a usable product only once at the end of a sequential process. This typically involves cross-functional collaboration among development, operational, and security interests to leverage constant feedback from the end-user in order to improve the functionality of the product through multiple iterations and provide constant support.

Application programming interface (API) - a set of definitions and protocols for building and integrating application software that enables applications to exchange data and functionality

Application software – a type of computer program that performs a specific function for an end-user

Blockchain - refers to the technological infrastructure and protocols that allow simultaneous access, validation, and record updating across a network in a decentralized manner. Blockchain technology is used with cryptocurrency and smart contracts, among other things

Bundled IT products and services - services offered as part of acquiring commercial off the shelf software (COTS), licenses, or cloud services that is separate but complementary to the acquired resource (e.g., training, maintenance, data conversion, reengineering, and rights to future upgrades and enhancements)

Cloud bursting – a configuration in which an application runs in a private cloud or data center and surges into a public cloud when the demand for computing capacity spikes during peak times

Cloud computing - 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.

Cloud service arrangement – a contract or agreement that provides a federal entity the right to access and use information technology resources provided by a vendor over the internet without the federal entity taking possession of the information technology resource on its own hardware or systems.

Commercial-off-the-shelf software (COTS) – ready-made application software that is purchased or licensed from a vendor to utilize the software as intended for internal-use

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,

Disclaimer: This material is presented for discussion purposes only; it is not intended to reflect authoritative views of the FASAB or its staff. Official positions of the FASAB are determined only after extensive due process and deliberations.

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.

Computer network – A set of computers that are connected for the purpose of communicating data electronically

Computer system – a combination of functional and related hardware and software components to perform a desired outcome

Computing infrastructure – consists of essential and foundational compute, storage, and networking resources required to operate and manage information technology environments. Examples include servers, data centers, and routers, operating systems and firewalls.

Computing platform - a group of technologies or that are used as a foundation upon which software applications are developed and implemented. Examples include coding language, middleware, database management systems, operating systems, application programming interface (API), and firewalls.

Cryptocurrency - a digital currency in which transactions are verified and records maintained by a decentralized system using blockchain technology, rather than by a centralized authority

Data conversion – the process of modifying and converting the format of data to transfer it to a more useful format based on a target system. Data conversion enables the data to be read, altered, and executed in an application or database other than that in which it was created

Data migration – the process of transferring data between formats or systems

Development, modernization, and enhancement (DME) - refers to projects and activities that lead to new IT assets/systems, or change or modify existing IT assets to substantively improve capability or performance

Enhancements – any modification that significantly increases computer system capabilities beyond its original functions

External-use software - software developed by an entity to be sold, licensed, or made publically available solely for the end user's needs

Hardware – refers to the tangible parts of computer systems that store and run instructions provided by software and makes the processing of data and supports baseline functions

Disclaimer: This material is presented for discussion purposes only; it is not intended to reflect authoritative views of the FASAB or its staff. Official positions of the FASAB are determined only after extensive due process and deliberations.

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)

Impairment - occurs when software or another IT asset no longer provides substantive service potential or a significant reduction occurs in the capabilities, functions, or uses of the asset prior to end of its estimated useful life

Information technology (IT) - the development, implementation, maintenance, and use of computer hardware, software, systems, cloud services, and networks to organize, communicate, and secure information electronically

Information technology security – a set of strategies, objectives, and methods used to prevent unauthorized access to an organization’s IT resources, such as hardware, networks, software, and data

Infrastructure as a service – 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).

Internet domain - An identification string that defines a realm of administrative autonomy, authority or control within the Internet

Internet domain name – The internet address of a website. Domain names usually end in a generic name such as .com, .org, or .gov.

Intranet – a network for sharing information, collaboration tools, operational systems, and other computing services within an organization, usually to the exclusion of access by outsiders

Internal-use software – acquired or developed software that is operated by an entity strictly for its own administrative, security, operational, or mission needs, with no intent of selling or licensing the software

Internally developed software - software that an entity is actively developing through internal employees, contractors, or a combination of both. This includes significant modifications that adds additional capabilities to new software and existing or purchased COTS software

Legacy modernization - rewriting or updating a legacy system to modern computer programming languages, architectures, data formats, software applications, or hardware

Disclaimer: This material is presented for discussion purposes only; it is not intended to reflect authoritative views of the FASAB or its staff. Official positions of the FASAB are determined only after extensive due process and deliberations.

platforms. Legacy systems are often modernized to maintain functionality, add features, or add security

Legacy system - an old technology, computer system, or application program relating to or being an outdated, inefficient, and/or incompatible computer system that is still in use and may pose inoperability and compatibility issues or risks to other systems without modernization

Load balancing – the process of distributing traffic and workloads across computing resources in a cloud environment to ensure that no single server or machine is under-loaded, overloaded, or idle.

Maintenance and repair – the process of monitoring, updating, and preserving software applications and IT infrastructure currently in use to sustain computer system security and operability without adding new capabilities or functions.

Operating system – the software that supports a computer system's basic operations by communicating with hardware and directing the processing of programs. Also called system software

Platform as a service - 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.

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.

Prototyping – the activity of creating working models of software applications used to gather end-user feedback for further design and implementation considerations for the final product. Prototyping can be utilized as part of agile development methods

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

Robotic process automation – software automation technologies that imitate mundane rules-based business processes traditionally performed by humans, such as extracting data, filling in forms, and moving files

Disclaimer: This material is presented for discussion purposes only; it is not intended to reflect authoritative views of the FASAB or its staff. Official positions of the FASAB are determined only after extensive due process and deliberations.

Shared service - a mission, operation, or administrative support function provided by a federal entity to other federal entities (interagency) or to separate components within the same entity (intra-agency)

Software - a set of instructions that tell a computer to operate and perform specific tasks. Software is often used to describe the intangible functional aspects of a computer and includes application and operating system programs, procedures, rules, and any associated instructions pertaining to the operation of a computer system or program

Software as a service – 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.

Software-hardware integrated asset – application software that is integrated into and necessary to operate general PP&E and does not serve another purpose separate from the hardware. Also referred to as “integrated or embedded systems”

Software in development – the accumulated cost of developing an internal use software asset that is not yet complete. Similar to construction in process (CIP) for PP&E

Software license - a legal instrument governing permissions and restrictions for use of a software application, source code, or related product. A software license is a product that gives the consumer various intellectual property rights over a vendor’s underlying software resource. The acquired license in this scenario generally allows the consumer to possess the underlying software resource on their own hardware and/or IT systems. A license can apply to individuals or entire organizations and can provide perpetual or term-based rights.

Thick client – Thick clients IT devices are full featured computers with all the standard hardware and locally installed operating system and applications.

Thin client - Thin clients are IT devices that connect remotely into a separate server or data center that does all the work in a virtual environment.

Update – a way to fine-tune a product to keep it running in an optimal manner. Software updates usually consist of small and frequent changes to correct security issues or coding bugs

Upgrade – A new version of software that replaces the old product and is used for significant changes and/or major improvements

Disclaimer: This material is presented for discussion purposes only; it is not intended to reflect authoritative views of the FASAB or its staff. Official positions of the FASAB are determined only after extensive due process and deliberations.

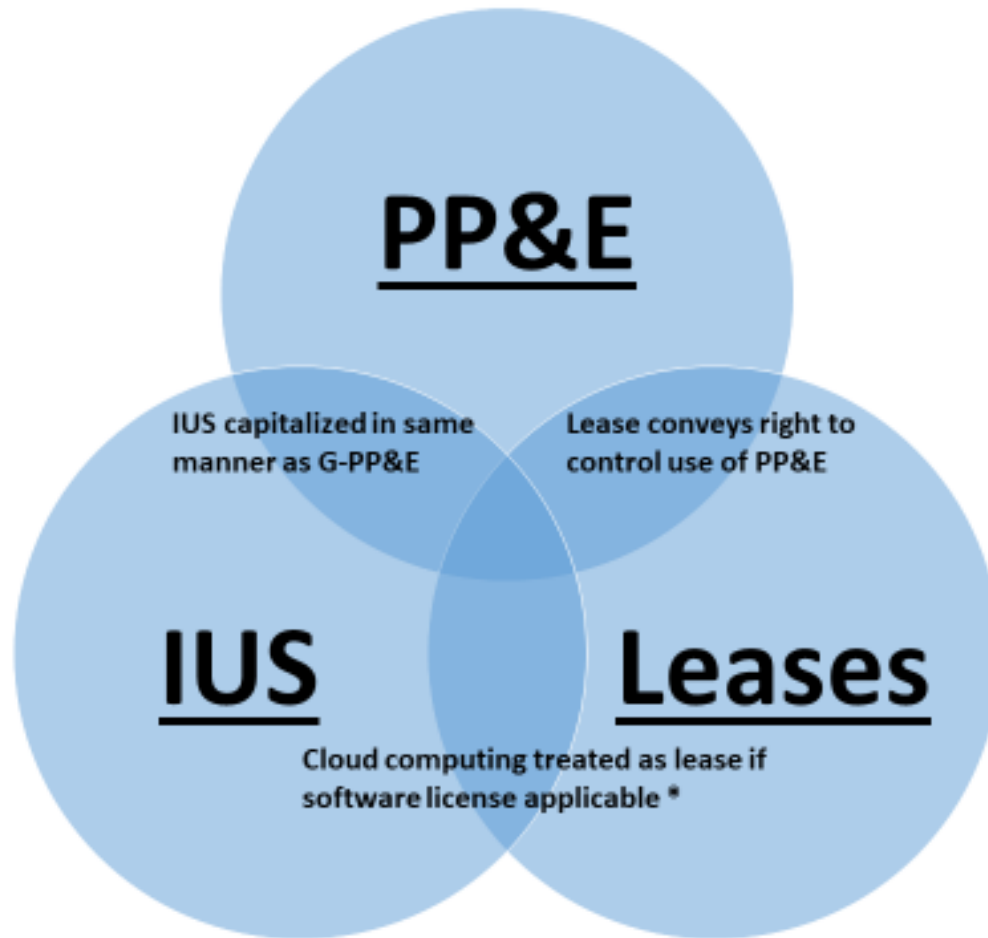
Waterfall development model – a non-iterative development method that breaks down activities into sequential and exclusive phases where each phase depends on the deliverables of the previous one and a usable product is produced after all phases occur. Also referred to as “Linear development model”

Web applications – an application software that is accessed through a website

Web page – a document written in hypertext that can be viewed by an internet browser

Website - collection of internally or publicly accessible, interlinked web pages that share a single domain name

Asset Guidance Framework



* The cloud computing arrangement guidance was applicable to the old capital lease guidance from SFFAS 5 and 6. Effective FY 24, SFFAS 54 scopes out software licenses from leases guidance, which will essentially make the TR 16 cloud computing arrangement guidance obsolete.

[illegible]