Cloud Tagging Strategy Guide

February 2, 2022

Office of Information Integrity and Access

General Services Administration
Office of Government-wide Policy

Table of Contents

Executive Summary 4

Introduction 5

- Intended Audience 5
- Purpose 5
- Structure 5

Overview of Cloud Tagging 7

- Cloud Tagging Definition 7
- Typical Cloud Resource Tags 7
- Tag Limitations 10

Approach to a Successful Cloud Tagging Strategy 12

- Overview 12
- Step 1: Establish the Goals for Your Cloud Tagging Strategy 12
- Step 2: Conduct a Stakeholder Analysis 13
- Step 3: Determine Your Tagging Requirements 15
- Step 4: Define Tags and Standardize Adoption 16
  - Tagging Conventions 16
  - Naming Conventions 17
  - Tagging Best Practices 19
  - Governance 19
- Step 5: Implement Tags Agency-Wide 21

Cloud Tagging Tools 23

- Cloud Management Platforms 23
- DevOps Tools 23
- Billing Tools 24

Primary Use Cases 25

- Cost Reporting 25
  - Technology Business Management 25
- Automation 31

Conclusion 32

Appendices 33

Appendix 1: Additional Resources 33

Appendix 2: List of Acronyms and Abbreviations 33

Executive Summary

Federal agencies face significant managerial challenges as they adopt increasingly complex cloud environments. However, without a cloud tagging strategy, they are unable to attain a comprehensive understanding of their cloud environments and are unprepared to address those challenges. Therefore, a cloud tagging strategy is essential for agencies to optimize their cloud utilization and costs.

The **Cloud Tagging Strategy Guide** aims to help agencies strategically approach their own cloud tagging efforts pertaining to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud solutions. The centerpiece of this guide is a recommended five-step process for developing a cloud tagging strategy, consisting of different managerial and technical considerations that build upon each other toward successful, agency-wide implementation. Beyond the aforementioned process, this guide brings the Federal IT community the most relevant information on cloud tagging tools and use cases, including Technology Business Management (TBM).

While this document provides guidance to inform your agency's cloud tagging strategy, cloud tagging, like other cloud capabilities, is continually and rapidly evolving. When your agency decides to create and refine its cloud tagging strategy, it is encouraged to evaluate the cloud tagging landscape beyond the pages of this document.

Introduction

Intended Audience

The intended audience for the Cloud Tagging Strategy Guide includes Information Technology (IT) system administrators, cloud architects, program and project managers, enterprise IT service managers, cloud financial and IT strategy analysts, contracting officers, and others adopting cloud as consumers.

Purpose

Agencies face significant managerial challenges as they adopt increasingly complex cloud environments built around hybrid cloud and multi-cloud architecture.[1] Without a cloud tagging strategy, they are unable to have a comprehensive understanding of their cloud environments and are unprepared to address those challenges. Therefore, a cloud tagging strategy is essential for agencies to optimize their cloud utilization and costs.

The purpose of the Cloud Tagging Strategy Guide is to provide your agency with high-level tagging guidance and examples that it can leverage and incorporate in its cloud strategy, in accordance with current Federal usage. It aims to help your agency develop and maintain an internal standard tagging schema at the enterprise level. While this document does not propose a government-wide tagging schema, such a schema may develop as a result of the recommendations provided here.

Cloud tagging is used in Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions. Consequently, this guide pertains to those solutions. Considerations concerning Software as a Service (SaaS) solutions are not covered here.

Structure

This document is organized into four primary sections.

1. **Overview of Cloud Tagging:** Defines and characterizes cloud tagging, and provides typical resource tags.

[1] Hybrid cloud architecture is the deliberate integration of public cloud, private cloud, and on-premises infrastructure. Though it is often mentioned as a form of multi-cloud architecture, multi-cloud architecture does not use on-premises infrastructure. A suggested reference for these concepts includes: Data Center and Cloud Optimization Initiative Program Management Office, Federal Cloud Strategy Guide: Multi-Cloud and Hybrid Cloud Guide (2021). CIO Council. https://www.cio.gov/assets/resources/Multi-Cloud%20and%20Hybrid%20Cloud%20Guide_v4_Final.pdf

2. **Approach to a Successful Cloud Tagging Strategy:** Describes a recommended five-step process for developing and implementing a cloud tagging strategy.
3. **Cloud Tagging Tools:** Reviews commonly used tools for cloud tagging.
4. **Primary Use Cases:** Presents cloud tagging use cases, including cost reporting and automation.

Overview of Cloud Tagging

Cloud Tagging Definition

A **tag** is a metadata label associated with an IT resource. **Cloud tagging**, then, is the process by which an organization defines and assigns labels to its cloud resources.[2] An organization can use cloud tagging to uniquely identify its cloud resources, and to organize, filter, and analyze its cloud resources and costs.

A given tag is made of two components: a **tag key** and a **tag value** that corresponds to the tag key. The tag key is the general metadata label under which specific tag values are categorized. For example, tag values associated with an `Environment` tag key may include `Dev`, `Test`, `Pre-Prod`, `QA`, and `Prod`, referring to development, testing, pre-production, quality assurance, and production, respectively.

Typical Cloud Resource Tags

Cloud tags generally fall into four tag categories:[3]

1. **Technical tags** identify and describe the operation of cloud resources.
2. **Business tags** track relevant roles, business units, and cost centers associated with cloud resources.
3. **Automation tags** are interpreted by automation tools to run processes on cloud resources.
4. **Security tags** track characteristics related to compliance and information security.

Beginning on the next page, **Table 1** provides commonly used tag keys along with corresponding categories, descriptions, and example tag values. The table is organized according to tag categories, which appear in the following order: technical, business, automation, and security. Note that **Table 1** is not exhaustive, and your agency is encouraged to find additional tags that will best serve its cloud strategy.

---

[2] CSPs also automatically generate tags to identify instances and subnets. These kinds of tags are not the focus of this guide.

[3] Access to the following reference requires registration on MAX.gov: Data Center and Cloud Optimization Initiative Program Management Office, Federal Cloud Strategy Guide: Agency Best Practices for Cloud Migration (2021). CIO Council. https://community.max.gov/display/Egov/Agency+IT+Modernization%3A+Educational+Resources+Building+Blocks

Table 1. *Commonly used cloud resource tags.*

Tag Key	Category	Description	Example Tag Values
`Name`	Technical	A descriptive name of the cloud resource.	`DataLake007`

`Environment`	Technical	Tag(s) to indicate the environment in which the cloud resource is used.	`Dev`
			`Pre-Prod`
			`QA`
			`Prod`

`Operations`	Technical	Tag(s) to identify a release version associated with the deployed cloud resource, instance increment in a refreshed immutable infrastructure, always on status.	`1.4`

`Purpose`	Technical	Tag(s) to describe the purpose of the cloud resource.	`App`
			`Database`
			`WebServer`

`Domain`	Technical	Tag(s) to provide the domain name of the cloud resource.	`gsa.gov` `cio.gov`
`OS`	Technical	Tag to identify the operating system (OS), including the OS version, to support the cloud resource.	`Ubuntu_21.04`
`Application`	Technical	Tag to identify an application, including the application version, on the cloud resource.	`COTS1.2` `Custom3.1`

`Tier`	Technical	Tag to identify the application architecture tier for a given multi-tier application on the cloud resource.	`1`
			`2`
			`3`

`Location`	Technical	Tag(s) to provide the CSP, data center, or data center location supporting the cloud resource.	`CSPName`
			`DataCenterName`
			`WashDC`

`License`	Technical	Tag(s) to identify the software licenses being utilized.	`VendorLicenseNumber`

Table 1, Continued. *Commonly used cloud resource tags.*

Tag Key	Category	Description	Example Tag Values

`CostCenter`	Business	Tag(s) to determine where the cloud resource should be billed notionally or actually, or to indicate the relevant accounting code or contract identification information.	`GSA_IT`
			`310510`
			`Contract340T`

`Owner`	Business	Tag(s) to identify the user or group who owns the cloud resource.	`SysPlanner003`
`Operator`	Business	Tag(s) to identify the user or group who is responsible for the operation of the cloud resource.	`SysAdmin050`
`BusinessUnit`	Business	Tag(s) to identify the business unit(s) that the cloud resource supports.	`HR` `Comms`
`Customer`	Business	Tag(s) to identify the customer base that the cloud resource supports.	`Vendors` `Employees`
`Compliance`	Security	Tag(s) to identify compliance-related information about the cloud resource.	`PII` `PHI`
`FedRAMP`	Security	Tag to identify FedRAMP impact level (low, moderate, or high) of the CSP associated with the cloud resource.	`FedRAMPhigh`
`FIPS`	Security	Tag to identify FIPS 140 Security Level (Level 1, Level 2, Level 3, or Level 4) of the CSP associated with the cloud resource.	`FIPS4`
`Schedule`	Automation	Tag(s) to identify the time at which the cloud resource operates.	`9AMto5PM` `WeekdaysOnly`
`Expiration`	Automation	Tag(s) to identify the time at which the cloud resource should be decommissioned.	`2022-11-30`
`Autoscaling`	Automation	Tag(s) to identify the cloud resource(s) automatically launched by autoscaling.	`Autoscaling`

For example, your agency may determine to use the following tag keys to label a given cloud resource:

- `Location`
- `OS`
- `Application`
- `Environment`
- `Tier`

These tag keys are the components of a cloud resource name. In combination, they create a simple template:

```
CloudResourceType-[Location]-[OS]-[Application]-[Environment]-[Tier]
```

Using the examples from **Table 1**, a virtual machine labeled with tag values may appear as:

```
VirtualMachine-CSPname-Ubuntu_21.04-COTS1.2-Dev-2
```

Tag Limitations

CSPs vary in the degree of flexibility they offer organizations seeking to implement a cloud tagging strategy.[4] For example, depending on the CSP:

- The maximum tag key length may range from less than 64 to over 256 characters;
- The maximum tag value length may range from less than 64 to over 512 characters;
- The characters are generally in either Unicode or alphanumeric format;
- Some special characters may be excluded;
- The maximum number of tags per cloud resource—that is, the unique combinations of a tag key and tag value for a cloud resource—may range from less than 10 to over 1,000;
- Tag keys may or may not be case sensitive; and,
- Untagged cloud resources may be permitted though are generally discouraged by CSPs. In some cases, untagged cloud resources cannot be tagged.

[4] Adekoya, O. J. (2020, January 27). *Multi-Cloud Naming, Tagging and Labelling*. Medium. https://medium.com/multi-cloud-management/multi-cloud-naming-tagging-and-labelling-9932a435ba98

Establish **Tagging Conventions** and **Naming Conventions** that are informed by limitations set by your CSP. If your agency uses multiple CSPs, ensure that the conventions accommodate the limitations of each.

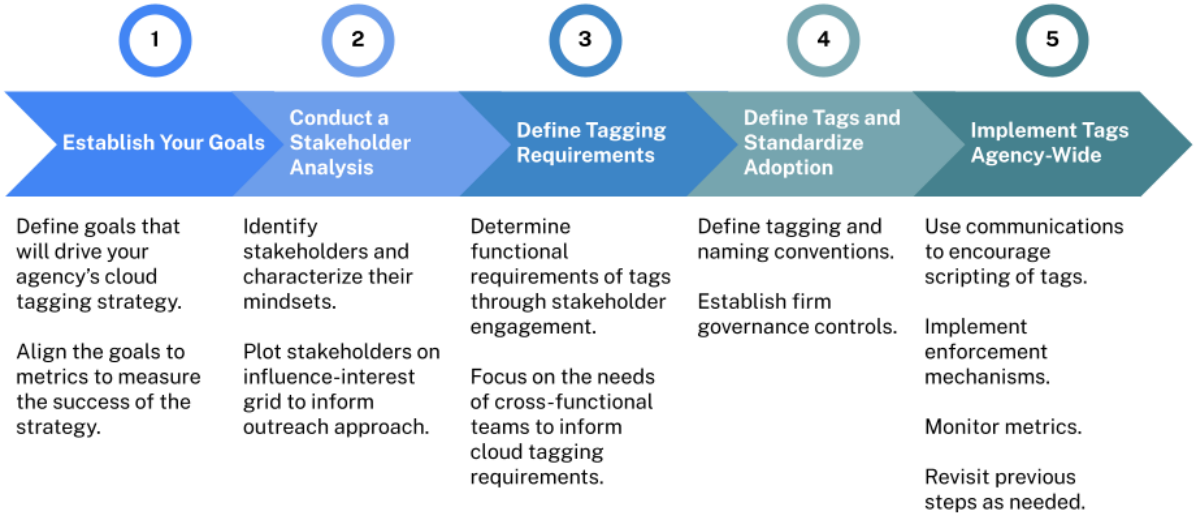
Note that, while CSPs also automatically generate tags to identify instances and subnets, these kinds of tags are not the focus of this guide.

Approach to a Successful Cloud Tagging Strategy

Overview

Agencies with an effective cloud tagging strategy can gain new insight into their cloud utilization and associated costs. Figure 1 shows the five-step process intended to help your agency navigate technical and organizational complexity, mitigate risk, and maximize these benefits.

Figure 1. *Five-step process for agencies to formulate and implement a cloud tagging strategy.*



The subsections that follow provide each of these steps in detail. Importantly, this process is not all-encompassing or fixed. Rather, your agency is encouraged to modify these steps in accordance with its mission, larger cloud strategy, and other organizational needs.

Step 1: Establish the Goals for Your Cloud Tagging Strategy

Tags are highly customizable according to the needs of cloud users. Within the broad scope of tagging possibilities, define goals that will drive your agency's cloud tagging strategy, address users' needs, and support your agency's larger cloud strategy. A logical continuation of Typical Resources Tags, cloud tagging goals generally fall into four categories: technical, business, automation, and security. Below are examples of each.

1. **Technical Goals:** Your agency can improve how efficiently it executes management tasks associated with a subset of cloud resources, or reduce the time needed to

debug applications by ensuring that the intended code is propagated to the relevant, deployed resources.[5]

2. **Business Goals:** Your agency may acquire a holistic view of cost allocation across environments, applications, users, or other custom tag keys. Furthermore, perhaps it aims to use that understanding, gained through tagging, to bill costs to the entities responsible for using cloud resources (i.e., chargeback).

3. **Security Goals:** Your agency may seek to enforce how it controls access to a subset of cloud resources by labeling users, roles, and the aforementioned subset with pertinent security tags.

4. **Automation Goals:** By using automation tags, your agency can automate routine tasks performed manually by IT staff, reducing overhead and increasing efficiency. For example, perhaps it seeks to automate when a cloud resource is decommissioned to minimize the time the resource is online.

Each goal should correspond to a metric to help you measure the success of your cloud tagging strategy. To help your agency arrive at its own tagging goals and metrics, **Table 2** provides example goals and corresponding metrics for each of the four categories. It is not an exhaustive list.

Table 2. *Example goals and metrics by cloud tagging category.*

Example Goal	Category	Example Metric
Increase the efficiency of management tasks associated with cloud environments.	Technical	Number of completed tasks per day associated with virtual networks that use tag-based conditions.
Bill cloud costs to the services responsible for using cloud resources.	Business	Total amount invoiced (in USD) to services via chargeback.
Increase enforcement of identity and access management (IAM) policies.	Security	Number of IAM policies implemented via tags.[6]
Maximize the number of tasks initiated via automation-related tags.	Automation	Number of tasks/processes initiated via command line scripts using automation-related tags.

[5] Access to the following reference requires a subscription to Gartner: Meinardi, M. (2019, December 12). Implementing a Tagging Strategy for Cloud IaaS and PaaS. Gartner. https://www.gartner.com/en/documents/3976255/implementing-a-tagging-strategy-for-cloud-iaas-and-paas

[6] Ibid.

Step 2: Conduct a Stakeholder Analysis

Conduct a stakeholder analysis to understand how stakeholders are impacted by the goals described in **Step 1: Establish the Goals for Your Cloud Tagging Strategy**.[7] Identify and categorize relevant stakeholders according to their level of interest and level of influence.

Figure 2. *Example of a stakeholder influence-interest grid.*

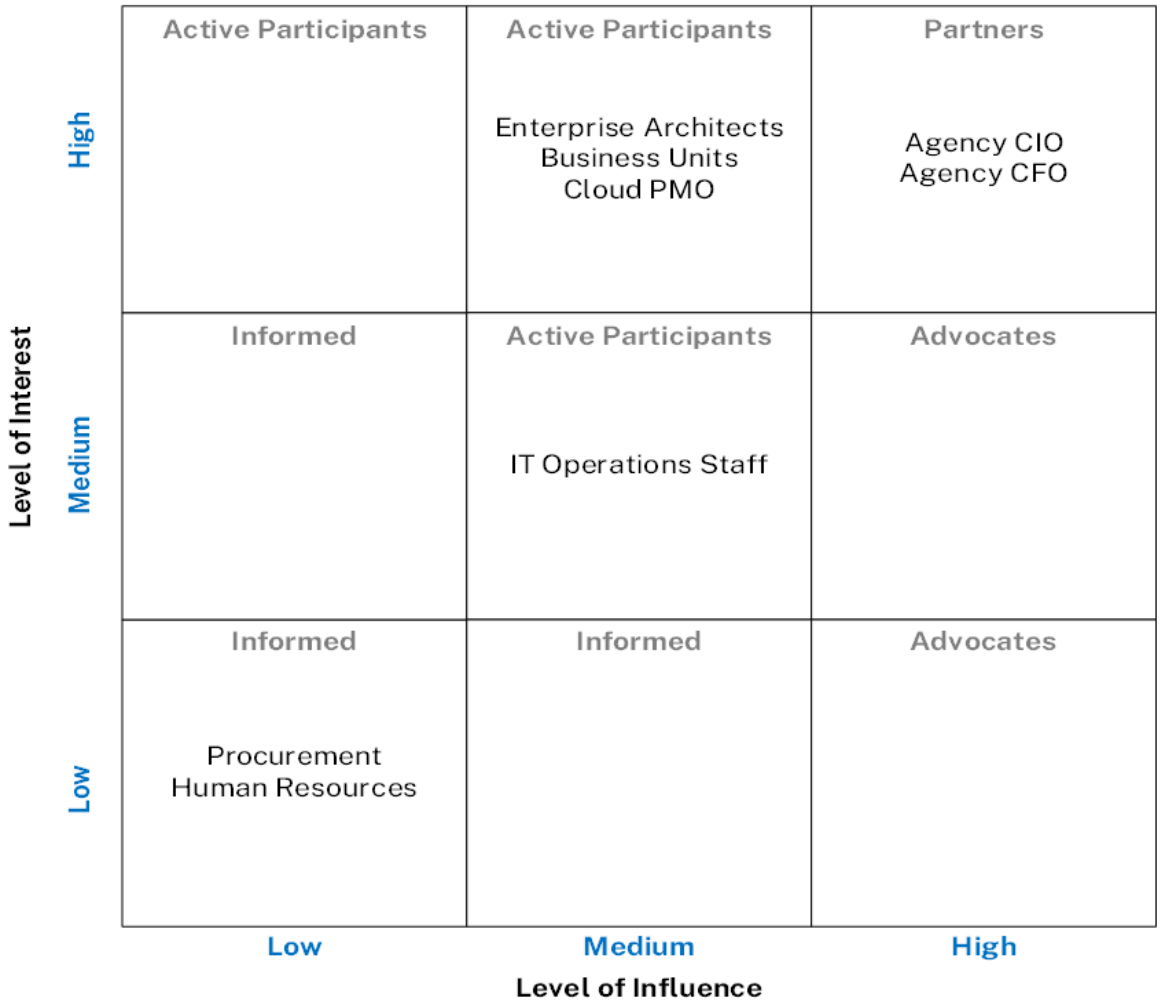


Figure 2 shows a stakeholder influence-interest grid, populated with examples of relevant stakeholders that in turn can be categorized as:

[7] Access to the following reference requires registration on MAX.gov: Data Center and Cloud Optimization Initiative Program Management Office, Federal Cloud Strategy Guide: Agency Best Practices for Cloud Migration (2021). CIO Council. https://community.max.gov/display/Egov/Agency+IT+Modernization%3A+Educational+Resources+Building+Blocks

- **Partners** (high influence, high interest) should be engaged and consulted regularly via executive briefings to inform decision-making pertaining to your agency's cloud tagging strategy.
- **Advocates** (high influence, low to medium interest) should be kept informed of recent progress.
- **Active Participants** (low to medium influence, medium to high interest) are directly impacted by a cloud tagging strategy and should be engaged directly to ensure their feedback is considered.
- **Informed** (low to medium influence, low to medium interest) stakeholders generally require only one-way communications via one-pagers, emails, and briefs.

In addition to placing stakeholders on the influence-interest grid, describe their objectives, characterize their attitudes, and reflect on how they may positively and negatively be impacted by your agency's tagging goals. Taken together, these insights will help your agency's cloud staging strategy address stakeholders' priorities and concerns.

While the stakeholder analysis initially occurs prior to the development of your tagging requirements, stakeholder engagement is continuous when creating your cloud tagging strategy. Make sure you vertically and horizontally align your agency, from C-level executives to operational staff, respectively, to the shared goals and attitudes you aim to achieve through the cloud tagging strategy (e.g., reduced cloud-related operating expenditures and improved utilization of cloud resources).

Step 3: Determine Your Tagging Requirements

Next, agencies need to arrive at the functional requirements upon which your agency's cloud tagging strategy depends. To determine these requirements, use the insights gained from **Step 2: Conduct a Stakeholder Analysis** and engage stakeholders to assess and document their tagging needs, with priority given to the observations from Partners and Advocates.

Functional requirements define the overall functionality of cloud tags. They include the tag keys and tag values needed by your agency's stakeholders, along with how tagging may be incorporated into reporting, compliance, and other administrative activities. Discussions with stakeholders, therefore, should center on answering simple and essential questions such as:

- What metadata associated with your cloud resources are most important?
- What tags create business value?
- What tags help provide a holistic view of your cloud resources?

- What metadata associated with your cloud resources are least important? In other words, what metadata about your cloud resources does not need to be tracked?
- What kinds of insights about your cloud resources do you want to gain? What tags should you use to gain those insights?
- Are you already using tags? If so, which ones?

Throughout your engagement with different stakeholders, focus on the needs of cross-functional teams to inform cloud tagging requirements, and emphasize the value proposition (e.g., cost savings, cloud utilization, reporting) relevant to each stakeholder. No one stakeholder or individual should be given disproportionate influence over what is and is not deemed a requirement, as this scenario would discourage others from sharing their observations and hinder the implementation of an agency-wide cloud tagging strategy.

Step 4: Define Tags and Standardize Adoption

First, refer to the cloud design documents offered by your agency's CSPs, which in many cases include a suggested cloud tagging strategy. These documents should serve as a starting point for defining and standardizing tags, not as a convenient workaround. Furthermore, if your agency uses multiple CSPs, find areas of overlap between recommended tagging and naming conventions, tag limitations, as well as recommended governance, to inform a coherent tagging strategy for your agency.

Tagging Conventions

Then, define the tag keys and tag values that meet the requirements from **Step 3: Determine Your Tagging Requirements**. Use **Table 3** as a starting point to establish tagging conventions for your agency's tag keys and values, and reach a consensus with stakeholders as to whether each is required, conditionally required, or optional. Formalize these conventions in a format similar to that in **Table 3**. As the table shows in the right column, a tag falls into one of three categories:

1. **Required tags** are tags that your agency's policy and governance deem mandatory.
2. **Conditional tags** are tags that your agency's policy and governance may or may not require, depending on whether a cloud resource has a particular tag. For example, if a cloud resource uses a particular combination of tag key and tag value, `Application: App2`, then the conditional `Compliance` key must be used along with a corresponding tag value, such as `PII`.
3. **Optional tags** are tags that your agency's cloud tagging policy and governance process do not require under any condition.

Note that Table 3 is intended to facilitate your own tagging conventions, rather than provide an exhaustive template for them.

Table 3. *Sample tagging conventions.*

Tag Key	Tag Values	Required/Conditional/Optional

`Purpose`	`Prod`
	`Mgmt`
	`IAM`
	`DB`
		Required

`Location`	`CSP1`
	`DataCenter1`
	`WashDC`
		Required

`Owner`	`johndoe@gsa.gov` `janedoe@gsa.gov`	Required
`Application`	`App1` `App2`	Required

`Environment`	`Dev`
	`Test`
	`Pre-Prod`
	`Prod`
	`QA`
		Required

`Compliance`	`PHI`
	`PII`
	`PCI`
	`Normal`
		Conditional; `Application: App2` processes sensitive personal data and requires `Compliance: PII`.

`BusinessUnit`	`HR`
	`Finance`
	`Shared`
		Required

`Expiration`	`2022-11-30` `2022-12-31`	Optional

Naming Conventions

Once tagging conventions are established, take a full inventory of your agency's cloud resources (both previously tagged and untagged) and facilitate additional discussions with stakeholders. For each cloud resource type, establish naming conventions that ensure they can be uniquely identified. Table 4 builds on Table 3 to provide example naming conventions for different types of cloud resource types. It is organized into four columns:

1. The type of cloud resource;
2. A prefix for the aforementioned cloud resource type;

3. A proposed format that begins with the aforementioned prefix and continues with tag keys relevant to the cloud resource type; and

4. An example of a tagging schema that uses tag values related to the aforementioned tag keys.

As with tagging conventions, your agency is encouraged, and indeed likely will find it necessary, to modify and expand on these naming conventions for its own cloud tagging strategy.

Table 4. *Sample naming convention schemas.*

Resource Type	Prefix	Possible Format	Example
Generic	`Prefix-`	`Prefix-[TagKey1]-[TagKey2]-[##]`	`Prefix-TagValue1-TagValue2-01`
Virtual Network	`Vnet-`	`Vnet-[Purpose]-[Location]-[Owner]-[##]`	`Vnet-DB-WashDC-john.doe@gsa.gov-02`
Subnet	`Snet-`	`Snet-[Purpose]-[Location]-[Owner]-[##]`	`Snet-DB-WashDC-jane.doe@gsa.gov-11`
Database	`DB-`	`DB-[Application]-[Environment]`	`DB-App1-Test-2022-12-31`
PaaS Application	`App-`	`App-[Application]-[Environment]`	`App-App2-Prod-PII`
Resource Group	`RG-`	`RG-[Application]-[Environment]-[##]`	`RG-App1-Prod-09`
Security Group	`SG-`	`SG-[Purpose]-[Compliance]-[##]`	`SG-IAM-PHI-05`
Data Lake Analytics	`DLA-`	`DLA-[Application]-[Environment]`	`DLA-App1-Prod`

Note that some formats end with a numeric scheme, in this case composed of two numbers, to help users interpret cloud resource names. Such a scheme may help users read and sort multiple resources with the same purpose (as in a cluster of them), or for a constantly recycled resource for security purposes (e.g., an increment count).

Tagging Best Practices

Consider the following best practices as you formalize your tagging and naming conventions:

- **Avoid concatenated tags.** Each field should have a separate tag to facilitate scripting with different combinations of tags. For example, within your tagging and naming conventions, ensure appropriate separation of tag keys and values (e.g., `Environment=Dev` and `Location=WashDC` rather than `[Environment=DevWashDC]`). Additionally, although name tags are often concatenated to help with identification in dashboards, each sub-element should also have a separate tag. The only tags that should be concatenated are those that are automatically created.
- **Consider character and visual limits in tags.** Make sure to select tag keys and values that will fit within the limit set by your CSPs. A common use case is a concatenated tag for the name of a cloud resource. While each individual tag uses fewer characters, a concatenated tag uses more characters and risks exceeding CSP-determined limits. To mitigate this risk, for example, use "dev" to denote a development environment instead of "development" if that tag will be used in a concatenated resource name.
- **Omit physical location information in the name tag key.** The physical location of a cloud resource can be included in a location tag that is automatically populated when the resource is launched.
- **Consider an alphanumeric scheme.** An alphanumeric scheme (e.g., `Prefix-[TagKey1]-[TagKey2]-[##]`) can help users read and sort through cloud resource names. However, if your agency uses Infrastructure as Code (IaC), consider using letters rather than numbers (e.g., `Prefix-[TagKey1]-[TagKey2]-[AB]`) to avoid the possible conversion of the scheme into real numbers.

Governance

As noted in the Cloud Strategy Guide, a cloud tagging strategy plays a key role in the governance of IaaS and PaaS platforms.[8] To fulfill that role, cloud tagging requires strong governance policies and practices to ensure that naming and tagging conventions are firm

[8] Access to the following reference requires registration on MAX.gov: Data Center and Cloud Optimization Initiative Program Management Office, Federal Cloud Strategy Guide: Agency Best Practices for Cloud Migration (2021). CIO Council. https://community.max.gov/display/Egov/Agency+IT+Modernization%3A+Educational+Resources+Building+Blocks

and widely adopted. Your agency is encouraged to establish governance that encompasses tag definitions, monitoring, and maintenance.

First, the definitions of cloud tags should be incorporated into your agency's governance processes. Definitions should identify and describe required, conditionally required, and optional tags for all cloud resource types and/or tag key-value combinations. For cloud resources that require many tags, consider creating a process flow diagram to guide users through the selection of the pertinent tag keys and tag values.

Next, decide and document how your governance controls should operate: preventatively, retrospective, or a hybrid of the two.[9] Preventative controls prevent users from tagging cloud resources with non-compliant tag keys and tag values. Most CSPs offer native capabilities to set and automate preventative controls through their provisioning tools, in which requests for cloud resources that have compliant tags can be approved, and those that lack compliant tags can be denied. In contrast, retrospective controls allow you to detect and address non-compliant tag keys and tag values after provisioning. Retrospective controls may either be soft (i.e., notifying users of tagging violations) or hard (i.e., deletion of the cloud resource with non-compliant tags). While preventative controls require fewer repetitive tasks performed by IT staff and, therefore, are generally the favored approach, your agency is also encouraged to incorporate retrospective controls because not all tagging violations can be addressed preventatively. For example, strong retrospective controls are needed for those CSPs that approve requests to provision cloud resources without first checking for non-compliant tags.

Agency-wide tags should be maintained by the same entity (i.e., division, office, or team) and use the same communication channels (i.e., email, group messaging, version control platforms like GitHub) as in the on-premise server environment to facilitate transparency across your agency's IT environment. However, because cloud tagging provides the assignment and usage of metadata far beyond server names, resources allocated to the process should be scaled accordingly.

Assure users that, while your agency's governance prevents users from creating new tags, the governance process ensures that the tags will adapt to their needs. As part of ongoing maintenance activities, build into your governance formal and/or informal mechanisms by which business units and other stakeholders provide input and insight into tag use, such as reviews of proposed changes via collaborative version control platforms (i.e. GitHub) and/or dialogues with stakeholders via agency-wide working groups, respectively. Assure users that, even if the governance denies certain tags, those tags are subject to change based on the needs of users.

---

[9] Access to the following reference requires a subscription to Gartner: Meinardi, M. (2019, December 12). Implementing a Tagging Strategy for Cloud IaaS and PaaS. Gartner. https://www.gartner.com/en/documents/3976255/implementing-a-tagging-strategy-for-cloud-iaas-and-paas

Step 5: Implement Tags Agency-Wide

Step 4: Define Tags and Standardize Adoption, as encompassed in your agency's governance, provides the foundation for **Step 5: Implement Tags Agency-Wide**. Implementation of your tagging strategy should rely heavily on a combination of communications and automation.

Thus far, you have engaged stakeholders to receive their comments on strategic goals, tagging requirements, standard nomenclature, and governance. Now that your agency has reached a shared understanding of these elements, the balance of communications begins to shift in the other direction. You must provide the cloud tagging strategy, including associated nomenclature templates and governance documentation, to all key stakeholders via your agency intranet, an IT office page, and the like. You must also notify stakeholders, at minimum, through email blasts and webinars, and ideally through the communication channels specific to their categorization in the stakeholder influence-interest grid (**Figure 2**).

Central to your messaging should be an enforcement date, at which time all preventative and retrospective controls are enforced.[10] Messaging should highlight both the benefits of tagging and, to realize those benefits, the need for users to incorporate agency-wide tagging and naming conventions into their cloud provisioning processes. Ensure that users have sufficient time (i.e., weeks to months rather than days) to familiarize themselves with the nomenclature and governance. If your messaging is successful, you should observe an increasing number of cloud resources with compliant tags as the enforcement date approaches.

Use IaC to implement tags across your agency's cloud resources. Generally, tags applied to a cloud resource should be scripted within the IaC scripts used to build environments. Possible exceptions to this approach include the development of the initial resources to build the IaC scripts or market research of a vendor product. While all non-development environments should have tags applied via IaC scripts, also consider integrating tags into development environment templates because any such tags would automatically appear when you provision cloud resources from those templates.

Beyond IaC, seek other ways to automate tagging of cloud resources. Query other sources of information to retrieve tag keys and automate tagging for the associated cloud resources.[11] Fully leverage the automation tagging features offered by your CSP, though be mindful of how these features vary across CSPs if your agency uses multiple CPSs.

---

[10] Access to the following reference requires a subscription to Gartner: Meinardi, M. (2019, December 12). Implementing a Tagging Strategy for Cloud IaaS and PaaS. Gartner. https://www.gartner.com/en/documents/3976255/implementing-a-tagging-strategy-for-cloud-iaas-and-paas

[11] Ibid.

Once implementation is underway, refer back to the original goals and metrics contained in your agency's cloud tagging strategy, as exemplified by **Table 2**. Is your agency's strategy helping your agency advance towards these goals and metrics as intended? Alternatively, have the goals and metrics changed since the strategy has been implemented? In either case, consider revisiting previous steps to continually reevaluate and realign the strategy. Commonly, part of that reevaluation process includes routine cloud billing reviews and cloud audits.

Cloud Tagging Tools

Cloud Management Platforms

Cloud Management Platforms (CMPs) provide users with unified management capabilities across public cloud, private cloud, and, in some cases, on-premises infrastructure.[12] CMPs feature a 'Dashboard' through which users can manage a multi-cloud or hybrid cloud environment. If your agency manages a hybrid or multi-cloud environment, strongly consider leveraging a cloud management platform (CMP) to apply tags to cloud resources. For example, to facilitate execution of agency's cloud tagging strategy, CMPs can:

- **Take an inventory of all cloud resources and corresponding tags.** The inventory can inform activities throughout execution of the cloud tagging strategy, from serving as a springboard for early discussions with stakeholders about different cloud resource types, to revealing untagged cloud resources during implementation.
- **Automate the tagging of cloud resources.** While cloud teams can apply tags via scripts (or manually), a CMP can provide and enforce standard tagging, as well as environmental maintenance, according to the needs of a large user base (i.e., the user base of a large agency).
- **Use tags to gather business intelligence.** A CMP can generate tried-and-true canned reports and visualizations from tags applied across your cloud environment. CSPs generally lack this out-of-the-box capability.

Importantly, small agencies and organizations could consider refraining from using CMPs if they find the native tagging capabilities of their CSPs to be sufficient. Additionally, while CMPs include 'Dashboard' through which to view and operate a cloud environment, in some cases, a 'Dashboard' may offer less sophisticated capabilities and therefore be less appealing than cloud native tagging capabilities.

DevOps Tools

DevOps refers to the combination and integration of activities related to software development and IT operations. DevOps tools can use tags to automate tasks related to software development and IT operations. They can automatically tag cloud resources as the tool orchestrates resources. For example, you can embed build number or code repository tags into standard templates, and then utilize tagging to create, deploy, and

[12] Access to the following reference requires registration on MAX.gov: Data Center and Cloud Optimization Initiative Program Management Office, Multi-Cloud and Hybrid Cloud Guide (2021). CIO Council. https://www.cio.gov/assets/resources/Multi-Cloud%20and%20Hybrid%20Cloud%20Guide_v4_Final.pdf

ultimately delete cloud resources built from those templates. Thus, the tags can propagate through the continuous integration/continuous delivery (CI/CD) pipeline.[13]

Billing Tools

Generally offered as a cloud-native application, billing tools can read tags to generate invoices for organization units. They can play a critical role in helping your agency monitor and optimize the costs associated with your cloud environment, establish accountability for cloud costs, and align to your agency's broader IT strategy. By interpreting tags, a typical billing tool can:

- Analyze costs according to cloud resource and billing entity (i.e., a cost center or business unit);
- Create invoices, financial reports, and other financial documents; and,
- Set recurring, spending thresholds for specific cloud resources and billing entities.

[13] Access to the following reference requires a subscription to Gartner: Meinardi, M. (2019, December 12). Implementing a Tagging Strategy for Cloud IaaS and PaaS. Gartner. https://www.gartner.com/en/documents/3976255/implementing-a-tagging-strategy-for-cloud-iaas-and-paas

Primary Use Cases

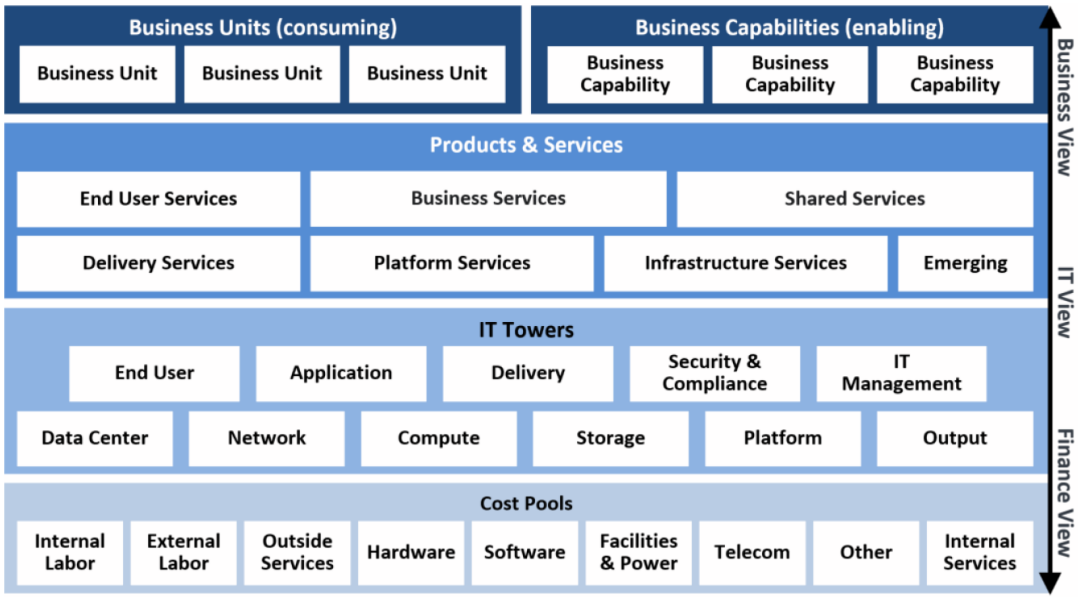
Cost Reporting

Cost reporting tags can be used to cross-reference CSP charges in any billing console against actual CSP invoices provided to your agency. They are commonly utilized to generate chargeback or showback costs to business units. Learn about how to use **Technology Business Management** (TBM) to implement consumption-based chargeback or showback. Furthermore, cost reporting tags can be used to ensure cloud resources are being properly managed by staff.

Technology Business Management

TBM refers to an approach to bring transparency to IT costs, consumption, and performance. Central to TBM is the allocation of costs throughout all layers of an organization, from cost pools (e.g., internal labor, software, hardware, facilities and power, among others) to business units and capabilities (**Figure 3**). This framework can help your agency improve cost efficiency of its cloud infrastructure, better align its resources to strategic priorities, maximize value on cloud-related and other IT investments, understand your existing IT environment to better prepare itself to leverage new cloud technologies, and help manage on-going operations. If your agency is interested in using TBM to help manage cloud costs, consider labeling cloud (i.e., IaaS and PaaS) and non-cloud solutions

Figure 3. *Diagram of the TBM Taxonomy.*[14]

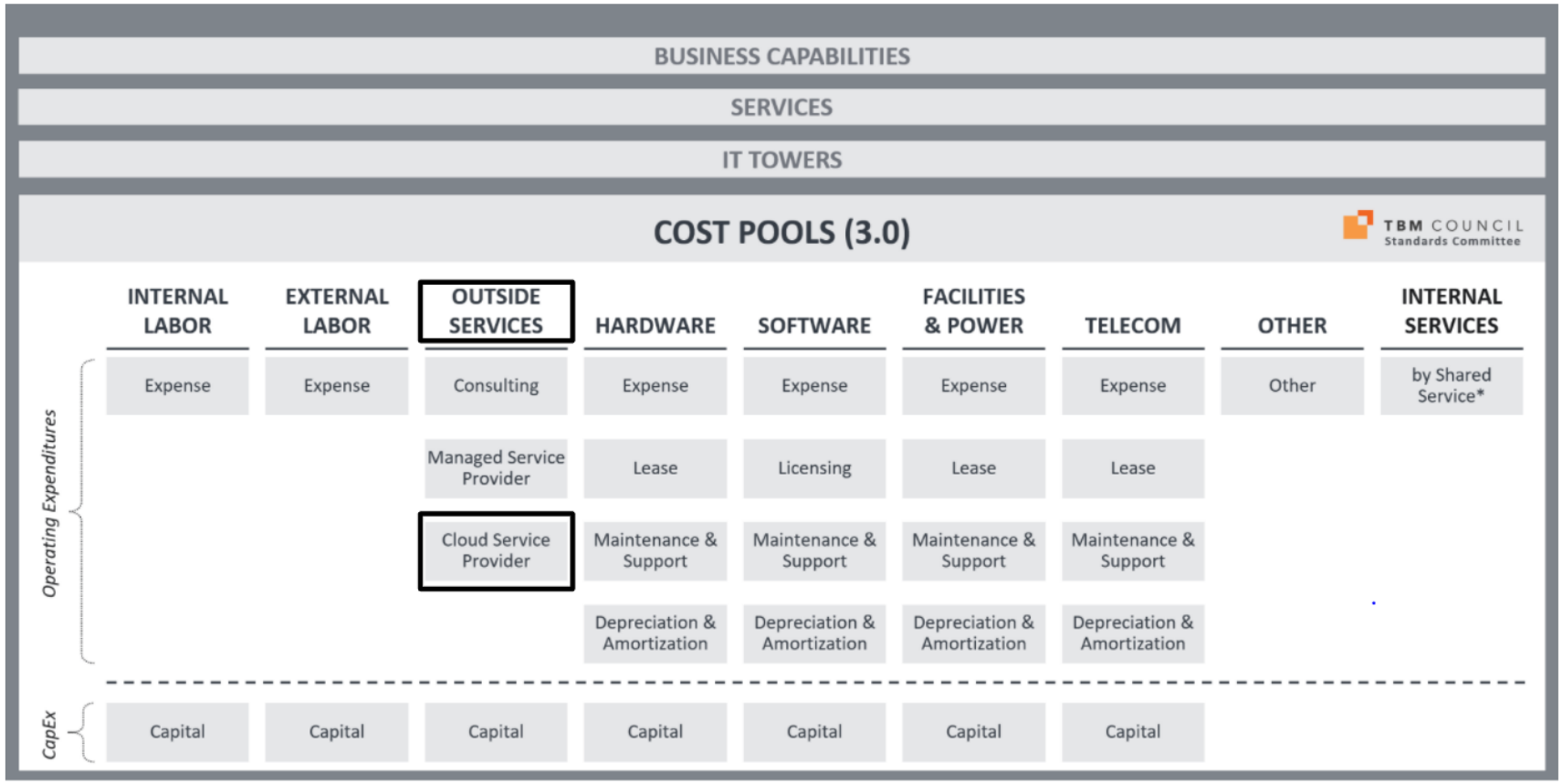


[14] Adapted from TBM Council, TBM Taxonomy Version 3.0.2 (2018, November 2). TBM Council. https://community.tbmcouncil.org/learn-tbm/tbm-taxonomy

with tags that can be traced back to the TBM Taxonomy. Note that these are generally standard tags that are needed to manage your technology solutions.

The costs of IaaS and PaaS solutions can be traced and translated through each layer of the TBM Taxonomy, from the cost pool layer to the business layer. To bring greater transparency to cloud costs through the stack of an IaaS and PaaS solution, the cost pool and tower layers can be further divided into sub-pools (**Figure 4**) and sub-towers (**Figure 5**), respectively. Additionally, **Figure 6** highlights product and service categories, and **Figure 7** highlights business units and capabilities. Taken together, these figures aim to provide your agency with tagging possibilities up the stack of an IaaS or PaaS solution.

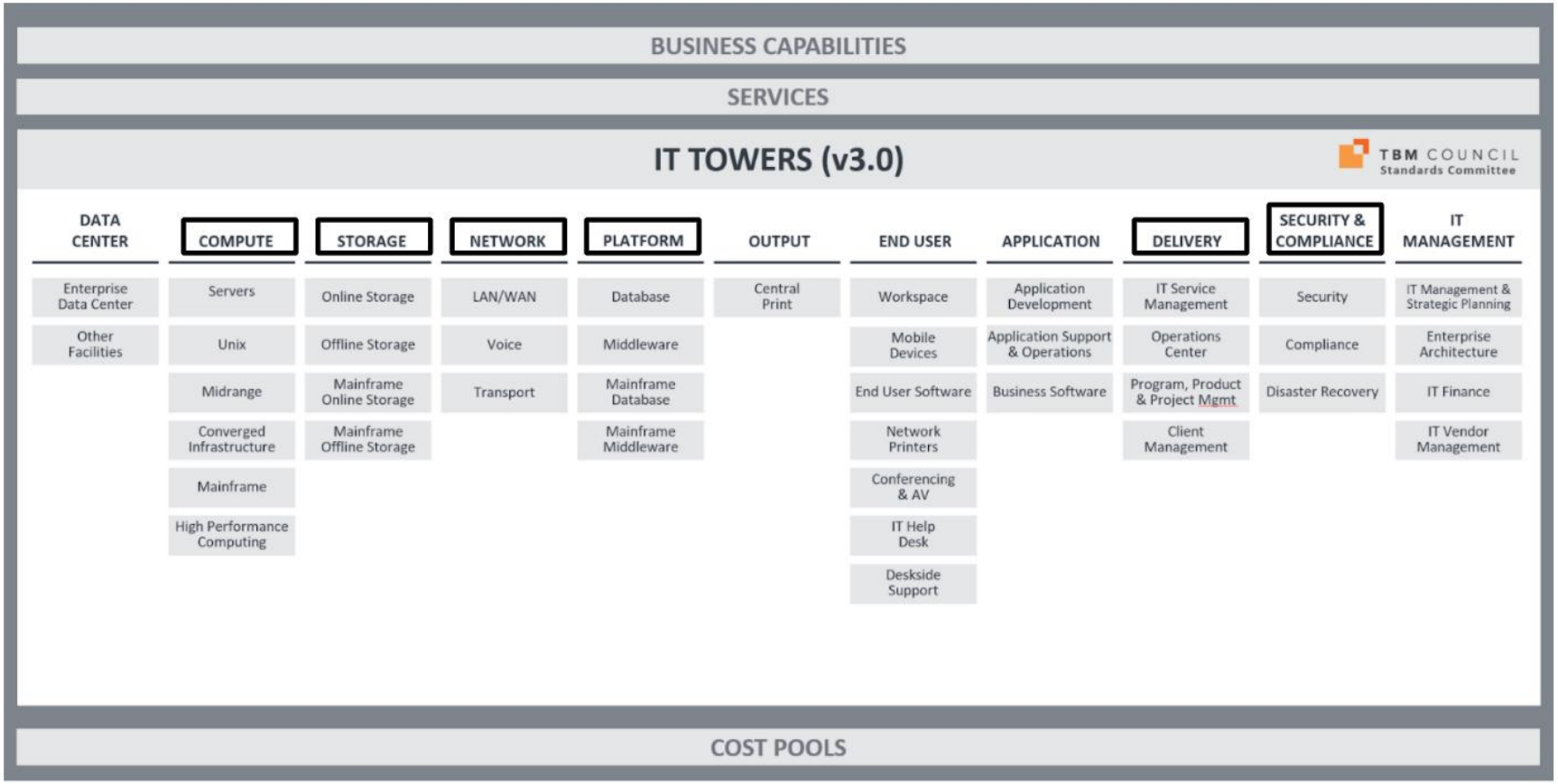
Figure 4. *Diagram of cost pools and cost sub-pools.*[15]



General ledger data pertaining to IaaS and PaaS solutions should initially be translated to the outside services cost pool and, in particular, to the CSP cost sub-pool, as highlighted by **Figure 4**. Thus, cloud resources should be tagged according to CSP.

[15] Adapted from Tucker, T. (2021, March 11). *Using TBM to Govern Enterprise Spending Inclusive of Public Cloud Services* [Webinar]. TBM4Cloud Workgroup Meeting. https://community.tbmcouncil.org/viewdocument/cloudtbm-workgroup-meeting-31121?CommunityKey=7485d5ff-1de4-4108-931e-b7787bcbc187&tab=librarydocuments

Figure 5. *Diagram of IT towers and IT sub-towers.*[16]

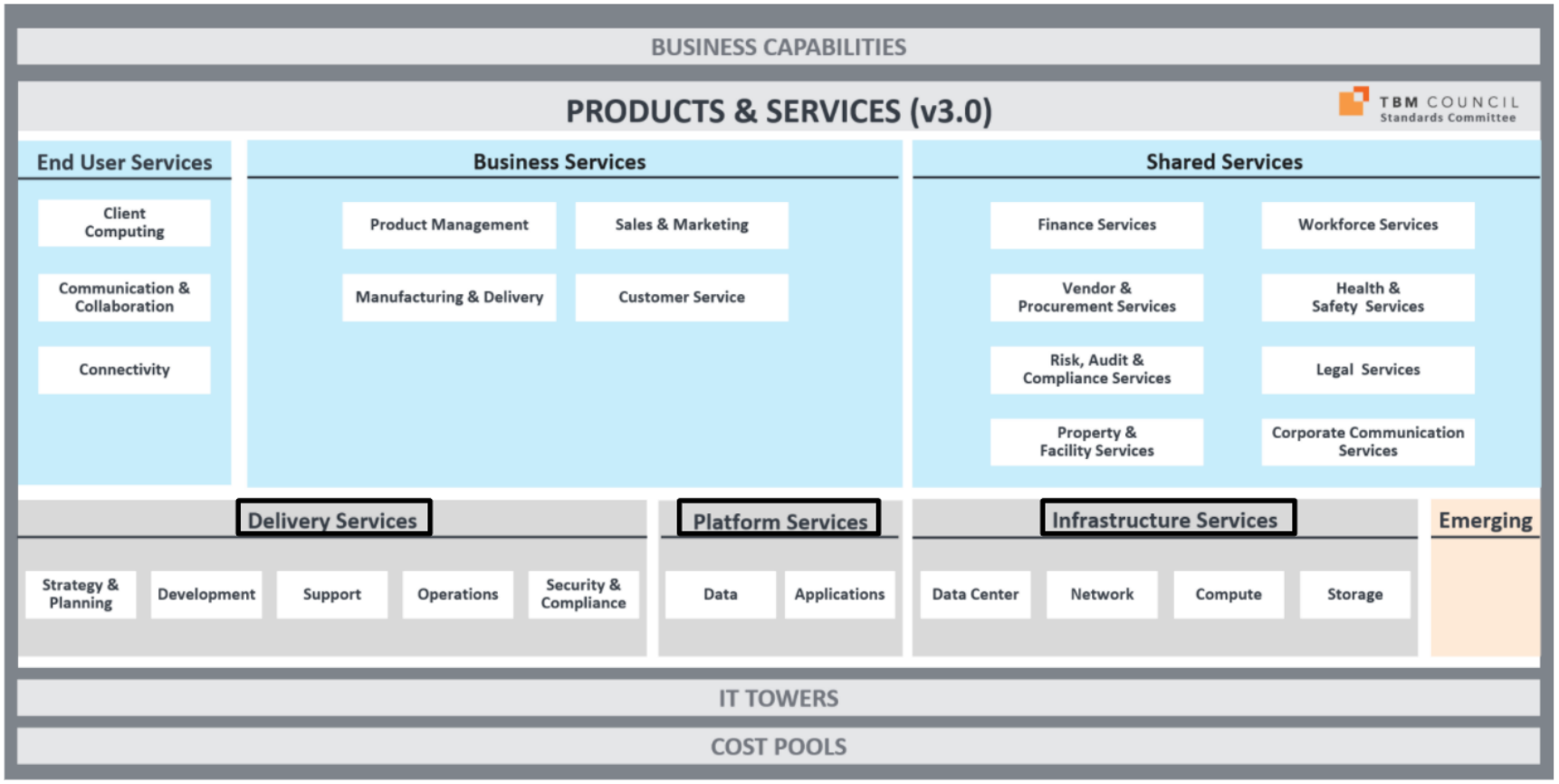


A single cost pool—in this case, outside services—may be translated to different towers, including compute, storage, network, platform, delivery, and security and compliance, as shown by **Figure 5**. Within each tower, a variety of sub-towers may be relevant to your agency's cloud tagging strategy, depending on its goals and metrics.

---

[16] Adapted from Tucker, T. (2021, March 11). *Using TBM to Govern Enterprise Spending Inclusive of Public Cloud Services* [Webinar]. TBM4Cloud Workgroup Meeting. https://community.tbmcouncil.org/viewdocument/cloudtbm-workgroup-meeting-31121?CommunityKey=7485d5ff-1de4-4108-931e-b7787bcbc187&tab=librarydocuments

Figure 6. *Diagram of service hierarchy.*[17]



IaaS and PaaS solutions may be categorized as technical rather than business solutions, and are thus located in the bottom half of **Figure 6** as infrastructure and platform services, respectively. Delivery services related to security and compliance, strategy and planning, and support, among others, may also be relevant to your agency's tagging strategy, again depending on

[17] Adapted from Tucker, T. (2021, March 11). *Using TBM to Govern Enterprise Spending Inclusive of Public Cloud Services* [Webinar]. TBM4Cloud Workgroup Meeting. https://community.tbmcouncil.org/viewdocument/cloudtbm-workgroup-meeting-31121?CommunityKey=7485d5ff-1de4-4108-931e-b7787bcbc187&tab=librarydocuments

its tagging goals and metrics. By tagging at the service level, for example, your agency can burden the actual costs of its IaaS or PaaS solutions with the internal costs associated with their operation.[18]

Figure 7. *Diagram of business units and business capabilities.*[19]

Your agency can then tag by business unit or capability to enable consumption-based chargeback or showback (Figure 7).

Table 5 shows example cloud tags that correspond to the layers of the TBM Taxonomy. CSP1 provides a compute platform via a virtual server for an HR department. To enable chargeback or showback, the `BusinessUnit` tag identifies the HR and IT departments, and is used with technical tags (`Service`, `ITTower`, `CostPool`) to track consumption data on the departments to make the chargeback or showback model more accurate. If the departments use the same number of cloud instances, then a tagging scheme would reveal that they should evenly divide the compute cost associated with the `Service` tag. Meanwhile, other departments that use CSP1 for networking, storage, or data center services would not be included in this calculation.

Table 5. *Example tags corresponding to the layers of the TBM Taxonomy.*

Layer	Sub-Layer	Example Tags
Business Units and Capabilities	Business Unit	`BusinessUnit=HR` `BusinessUnit=IT`
Services	Infrastructure Services / Compute	`Service=InfrastructureCompute`
IT Towers	Compute / Servers	`ITTower=VirtualServer`
Cost Pools	Outside Services / Cloud Service Provider	`CostPool=CSP1`

[18] Version 4.0 of the TBM Taxonomy calls the components of this layer "solutions," an update from the "products and services" from Version 3.0.2.

[19] Adapted from TBM Council, TBM Taxonomy Version 4.0 (2020, December 16). TBM Council. https://higherlogicdownload.s3.amazonaws.com/TBMCOUNCIL/c15d372f-9951-46c8-9c3f-213c696401b6/UploadedImages/TBM_Taxonomy_V4_0.pdf

Automation

As noted throughout this guide, consider tagging cloud resources with automation scripts. Table 6 is an excerpt of an example comma-separated values (CSV) file that can be used in conjunction with migration scripts. Through a command line interface, you can initiate a migration process that will read the CSV file to migrate on-premises virtual machines (VMs) to a CSP. Data on the on-premises and cloud environments fall under the beige and gray column headings, respectively.

The migration script can automatically assign the tags listed in the tags column to the migrated VM. While this example provides only one VM, a CSV file like this may contain hundreds of VMs that will migrate and receive automatically assigned tags.

Note that column headings and values in this CSV file are fictitious and not intended to be used in conjunction with a migration process.

Table 6. *Excerpt of CSV file with tag field populated with tags.*

Application Information Brief		Development Environment				
UniqueID	Normalized Application Name	VMs	VM IP Address	VPC Name	VPC ID	Tags
130	App1	DC1-E-MBAMSQL2P	10.150.205.59	GSA Dev	vpc-2c12cc31	ApplicationName=App1 Owner=johndoe@gsa.gov CreationTimestamp=YYYY-MM-DD HH:MM:SS Environment=Int Tier=2 BusinessUnit=Shared Location=WashDC Domain=gsa.gov Purpose=Database

Open **Attachment 1** for the full CSV file.

Conclusion

While cloud tagging is only one of a multitude of cloud-related topics, its importance to your agency's IT modernization efforts should not be understated. Indeed, your agency's cloud tagging strategy will not only bring clarity to its cloud utilization and costs, but also play a critical role in its larger cloud strategy. With this guide, your agency can thoughtfully and confidently pursue a cloud tagging strategy on the path to a comprehensive cloud strategy.

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

Appendices

Appendix 1: Additional Resources

- Application Lifecycle Framework
- Application Lifecycle Framework Templates
- The Application Rationalization Playbook
- Cloud Strategy Guide*
- Cloud Strategy Artifacts*
- Small and Micro Agency Cloud-Strategy Toolkit*
- Multi-Cloud and Hybrid Cloud Guide
- Technology Business Management Playbook
- TBM Taxonomy Version 4.0

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

Appendix 2: List of Acronyms and Abbreviations

Abbreviation	Meaning
CI/CD	continuous integration/continuous delivery
CMP	cloud management platform
Comms	communications
COTS	commercial off-the-shelf
CSP	cloud service provider
CSV	comma-separated values
DB	database
DCCOI	Data Center and Cloud Optimization Initiative
Dev	development
DevOps	development and operations
DLA	data lake analytics
FedRAMP	Federal Risk and Authorization Management Program

Abbreviation	Meaning
FIPS	Federal Information Processing Standards
HR	Human Resources
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	identity and access management
IT	information technology
ITSM	information technology service management
Mgmt	management
OS	operating system
PaaS	Platform as a Service
PHI	protected health information
PII	personally identifiable information
PMO	Program Management Office
Pre-prod	pre-production
Prod	production
QA	quality assurance
Rg	resource group
SaaS	Software as a Service
Sg	security group
Snet	subnet
SysAdmin	system administrator
SysPlanner	system planner
TBM	Technology Business Management
VM	virtual machine
vnet	virtual network