U.S. PUBLIC SECTOR FINOPS PLAYBOOK

Version: 1.0

FinOps Foundation

Table of Contents

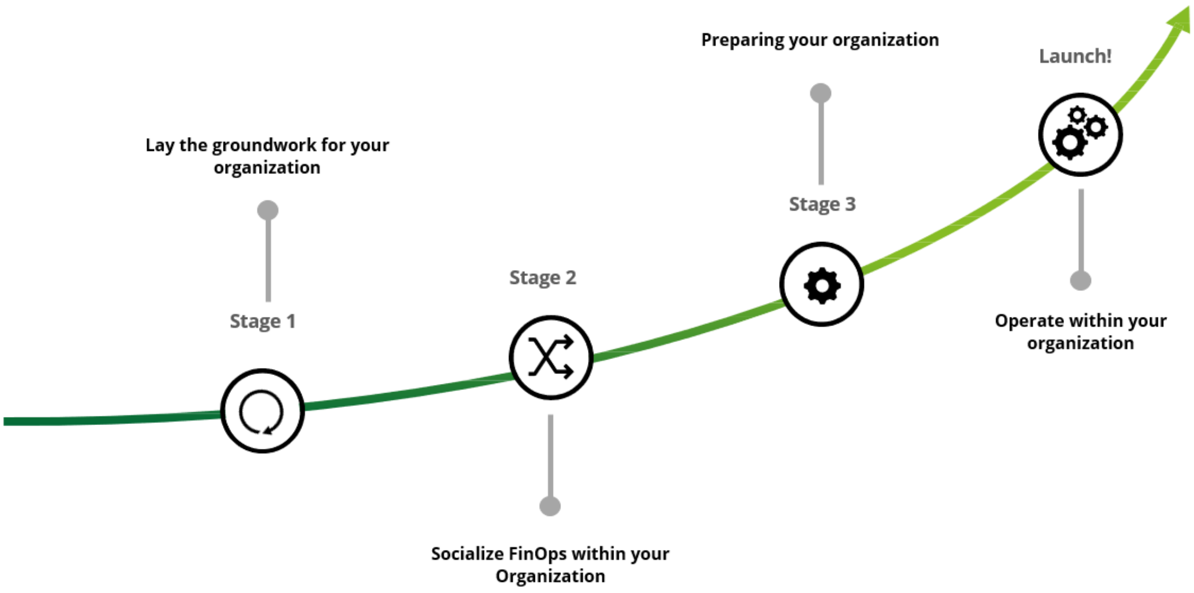
Table of Contents 1
Introduction 2
FinOps Basics 3
Key Terms 3
Disclaimer 4
Stage 1 4
Planning for FinOps in an Organization (Laying the Groundwork) 4
Do your research 5
Create a plan 6
Bring cultivated supporters together 8
Perform Initial Resourcing 8
Stage 2 12
Socializing FinOps for adoption in an organization 12
Defining the Initial FinOps Model 14
Creating your Cloud Strategy 14
Automation 15
Creating your Tagging Strategy 16
Aligning Consumption to Funding Sources (Showback and Chargeback) 18
Commitment-based Purchases & Timing 18
Identifying Tools and their Benefits 19
Cloud Native Application and Tool Considerations 22
Amazon Web Services Native Services 22
Azure Native Services 24
Google Cloud Native Services 25
Forecasting and Budgeting for Cloud 26
Acquisition of Cloud 27
Stage 3
Preparing the organization for FinOps 27
Assess FinOps Readiness 28
Engage Stakeholders 28
Begin Operating with FinOps 29
Keep Maturing your FinOps Implementation 29
Acknowledgements 30

Introduction

FinOps is an evolving cloud financial management discipline and cultural practice that enables organizations to get maximum business value by helping engineering, finance, technology and business teams to collaborate on data-driven spending decisions.

This playbook is designed to build upon the existing FinOps framework to assist federal agencies as they begin (or mature) their cloud journey. While each agency should tailor their FinOps implementation to their organization's current state and desired outcomes, this playbook highlights areas within the FinOps framework which will likely be slightly tailored for a public sector use case. It is our greatest hope that this playbook will help guide federal agencies towards a successful cloud financial management practice, enabling key outcomes afforded by near real-time cloud spend visibility and reporting of executive level details to align an agency's cloud operations with strategic goals.

This playbook is organized into three stages which are designed to assist in setting up your agency in implementing FinOps, allowing you to smoothly transition into operating FinOps within your organization.


Lay the groundwork for your organization
Stage 1
Stage 2
Socialize FinOps within your Organization
Preparing your organization
Stage 3
Launch!
Operate within your organization

While this playbook follows a sequential, start - finish look to implementing FinOps, at its core, FinOps involves consistent, cyclical actions that can be implemented at any time and any stage during the cloud adoption process. Crawl, Walk, Run is a consistent theme with FinOps and we hope that regardless of where you are in your cloud adoption journey, this playbook will provide value in either building or optimizing your FinOps organization.

FinOps Basics

At its core, FinOps is a cultural practice. It's the way for teams to manage their cloud costs, where everyone takes ownership of their cloud usage supported by a central best-practices group. Cross-functional teams in Engineering, Finance, Procurement, Product, etc. work together to enable faster product delivery, while at the same time gaining more financial control and predictability.

This public sector FinOps Playbook builds upon the FinOps Framework and the Adopting FinOps roadmap and it is useful to develop an understanding of FinOps as a practice overall as you are using this playbook. An introductory video and a wide array of information on the FinOps Framework is available at the links above. Free introductory training on FinOps is available via EdX. We recommend those using this playbook establish a baseline understanding of FinOps, its Principles, and its practice prior to using this playbook.

Key Terms

Tagging (or Metadata) The process by which an organization defines and assigns tags, labels, or other metadata to its cloud resources. GSA provides a great Cloud Tagging Strategy Guide which is available CIO.gov.

Showback The ability to show charges to the product, department or other hierarchical grouping that is responsible for them, while managing payment of expenses from a centralized budget

Chargeback The ability to take the charges each department or chosen hierarchical grouping (such as application or system) and sending those expenses to the entity (or its accounting system) for payment

Persona Represents a user-type within the FinOps discipline such as “Contract Persona,” “Engineering Persona,” “Finance Persona” etc.

Unit Economics Practice of measuring cloud spend against a business metric (total revenue, service provided, completed tasks/orders, etc) rather than simply looking at the cost in isolation

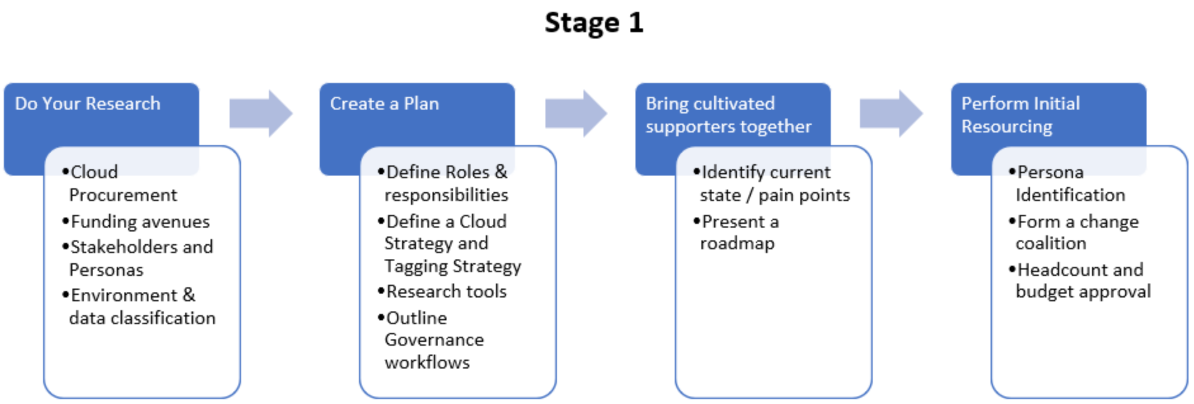
Commitment-based Discounts Purchase of the right to use certain cloud resources with discounted prices in exchange for a commitment to use either a minimum level of resources or spend a minimum amount, for a specified term of one or three years

Disclaimer

This playbook was developed by a working group within the FinOps Foundation (www.finops.org) with input from key federal IT practitioners and industry representatives. This document should not be interpreted as official policy or mandated action, and does not provide authoritative definitions for IT terms. Rather, this playbook is designed to supplement existing federal policy on cloud use, and to provide helpful guidance on managing cloud use in the public sector.

Stage 1

Planning for FinOps in an Organization (Laying the Groundwork)


Stage 1
Do Your Research
•Cloud Procurement
•Funding avenues
•Stakeholders and Personas
•Environment & data classification
Create a Plan
•Define Roles & responsibilities
•Define a Cloud Strategy and Tagging Strategy
•Research tools
•Outline Governance workflows
Bring cultivated supporters together
•Identify current state / pain points
•Present a roadmap
Perform Initial Resourcing
•Persona Identification
•Form a change coalition
•Headcount and budget approval

It is important to note here that if you are planning for a FinOps function in your organization, you may be doing so for an entire agency, for a component of that agency or even for a single cloud contract. In a public-sector context, FinOps may be more complex to implement the wider the scope of its control. There are obvious and important benefits to having FinOps be managed as high in an organization's hierarchy as possible, in order to develop consistent cloud management techniques, but the practical realities of cross-contract and agency-wide coordination can be daunting in public sector organizations. As we do in other areas of FinOps, you can start small, and build from success, but be ever mindful to coordinate across organizational boundaries wherever possible to achieve greater efficiency.

Do your research

An effective FinOps adoption plan consists of determining the current state and painting the future-state. Consider the current organization, stakeholders, financial systems, business models, and processes already in place. Seek out the right stakeholders within the organization. Provide information on how the implementation of FinOps will help alleviate the issues facing various teams within your agency. As an individual looking to bring FinOps to your organization, you will need senior level sponsorship as well as cultivated supporters to build momentum.

Identify and Document:

- Possible Advocate/Champion/Executive Sponsor, and have one-on-one conversations with each of them using a customized FinOps introduction deck or initial interview questions to determine adoption strategy.
- Pain points being experienced by the organization during your conversations, such as cloud costs breaking business cases, general perception of cost overruns, lack of cost visibility by cloud consumers, etc.
- State of cloud procurement in your organization or in other organizations in order to learn from their experiences.
- Funding avenues with your budget stakeholders, and possible contract vehicles to explore within and outside your agency with your acquisition stakeholders.
- Who will be the key individuals responsible for administering any resultant contracts. What tools do they have or will they need to be successful?
- Impacted groups, teams, and individuals during your conversations. Who is affected by the pain points?
- Know your environment classification. Understand the classification of data and any potential security requirements which can affect tool selection, tagging taxonomy, and cloud service provider

Create a plan

Utilizing the information outlined above, paint the picture of the future state and create a plan to implement the necessary changes in applicable areas. This should include the future state of your cloud organization as well as your cloud environment. By considering both, it will allow the creation of a set of governance & organizational processes which will support your cloud goals. Additionally, considering the end state of your cloud environment will allow for the planning of resources and tools to support your overall goals.

- The Adopting FinOps deck (available from the FinOps Foundation) is a good starting point for this plan, but must be customized for the organization, the personas being approached, the pain points, and the culture.
- Education on FinOps as well as clear roles and responsibilities of the governance and organization are key foundation points for your plan.
- Identify tool requirements. Determine if existing tools can fill the needs of the plan both in the current and future state. See Identifying Tools and their Benefits for specific considerations for tool selections and cloud native considerations
- Identify an organizational "home" for the FinOps function. This may be in a Cloud Center of Excellence (CCoE), Capital Planning Office, PMO, in Chief Financial Office (CFO), or in IT. Depending on the complexity of the organization structure, creating a dedicated FinOps team might take a phased approach. Some organizations might
    - Set up a cross-functional transformation program office and create workstreams / working groups,
    - Create a FinOps function as part of the extended Cloud Business Office / Cloud CoE
    - Evolve into a dedicated Cloud FinOps Team.
- Take into consideration who the contracting officer's representative (COR) is and what their role will be within the FinOps team. This can be particularly challenging when looking at cloud spend across multiple contracts, or at an agency-wide level.
- Identify candidate early-adopter teams
    - Ensure these teams represent a cross-section of your organization to include IT, Finance, Executives and others. Having only one type of team represented may lead to "group think" and you'll miss out on important perspectives.
- Identify KPIs that will be used to measure the FinOps function as well as ways to measure engagement and performance of stakeholders like business units and

application teams. Note: These are preliminary and will evolve during Stage 2, but it’s important to have a starting set

- Prepare a communication plan that will be used in Stage 2

Bring cultivated supporters together

…and explain why it is important to adopt FinOps. Your cloud journey will span a variety of personas and stakeholders from issuing an RFI, looking at contract/procurement vehicles, deciding your Cloud Service Provider, to implementing your cloud migration or new stand-up environment. FinOps becomes a conversation to have with these stakeholders and should become a part of your overall Cloud Strategy.

- Highlight current state, pain points, and other potential challenges
- Identify threats and show scenarios that could happen if action is not taken (tie to agency goals, mission objectives, agency compliance requirements)
- Demonstrate what Crawl, Walk, Run would look like for the organization
- Examine opportunities that should be, or could be, exploited
- Present the roadmap
    - Get feedback from the executive sponsor(s) and adjust as needed
    - Including initial team size, budget, timeline for initialization
    - Value proposition (e.g. ROI such as the cost of having a FinOps function vs. an ongoing cloud overspend)
- Present to other stakeholders, supporters, and a pilot set of new people such as business unit leads

Education and collaboration are the foundation of a successful FinOps implementation in the public sector. Cloud (and technology in general) is constantly changing and evolving; the ability to have a procurement vehicle, contract, and buy-in from stakeholders will ensure that your cloud strategy can remain dynamic with those changes.

Perform Initial Resourcing

When proposing the adoption of a FinOps function within an organization, there will be a need to brief a variety of personas among the executive team to gain approval, buy-in, and involvement in conducting FinOps and achieving its goals. Consider each Persona and stakeholder that is necessary in some of the below actions:

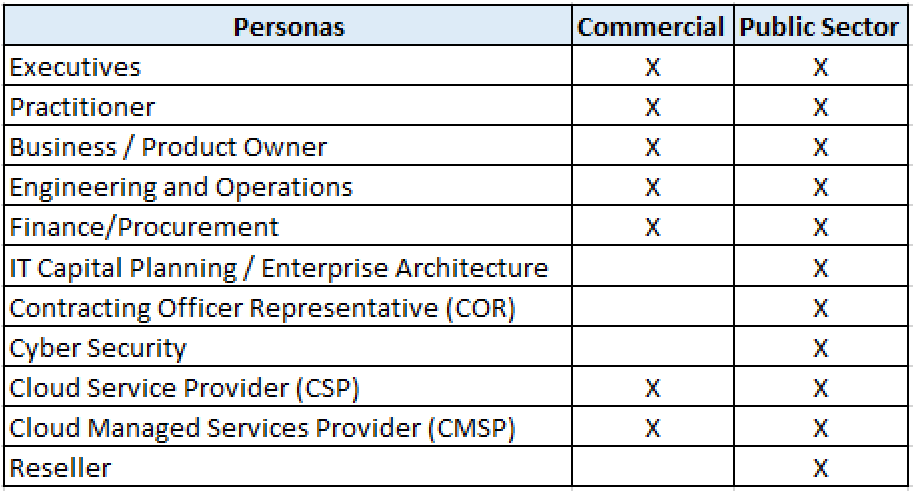
- Request support from sponsor(s) to recruit other executive leaders as advocates
- Define the goals of the FinOps teams and the members (Cloud Charter)
- Form a change coalition (true org. Influencers & stakeholders)
- Get budget approval, headcount, matrixed involvement from related groups
- Procure new tools or contract support for FinOps (if appropriate at this stage of the roadmap)

FinOps Personas within the public sector may align with commercial, but some personas may have the same title but have different priorities or some personas are new and specific to the public sector. As an example, in commercial companies, important procurement functions are often handled entirely by the Finance organization, where in the public sector, procurement is often a separate group with an important and mandatory set of responsibilities and personal liabilities. So a COR persona, and a CO persona who are not as connected with the business results the agency is attempting to gain from cloud must typically be thought of as stakeholders in the public sector. Tailor the Personas your FinOps team might support to be specific to your organization.

Additionally, if at any point a Persona is employed as a contractor supporting the FinOps efforts within your organization, you should understand the terms of their contract. Reach out to your acquisition team to ensure the proper language regarding nondisclosure of acquisition and financial data protects the confidential information one may come in contact with as a part of their work. Understand what abilities they may have to create policy or procedures which are binding upon other contractors working in other areas of the organization and using cloud.

The table below contains some examples of differences in Personas between the commercial and public sector.

Below is a breakout of the Public Sector personas or differences between overlapping personas.



Personas	Commercial	Public Sector
Executives	X	X
Practitioner	X	X
Business / Product Owner	X	X
Engineering and Operations	X	X
Finance/Procurement	X	X
IT Capital Planning / Enterprise Architecture		X
Contracting Officer Representative (COR)		X
Cyber Security		X
Cloud Service Provider (CSP)	X	X
Cloud Managed Services Provider (CMSP)	X	X
Reseller		X

Executives: A traditional commercial executive persona typically is concerned with accelerated growth, faster time-to-market, meeting budgets, and revenue growth. However, an executive persona in the public sector may be concerned less with revenue and more with forecasting and budgeting, adherence with federal and agency-specific mandates, and cumulative spend. This persona would reside within the CIO. Information containing spend to date tied to outcomes/projects as well as potential cost savings will be particularly helpful to gather.

Finance/Procurement: A traditional procurement persona may be one or two persons within your organization. However, within the public sector there will be several additional personas to consider. These individuals may require an overview of cloud consumption versus existing on-premise infrastructure. Having a recurring and frequent cadence with your finance, procurement, and contracting personas is key for a successful FinOps implementation in the public sector. How you fund, solicit, award & administer your cloud contracts will largely depend on how much the personas within this area understand the cloud needs in order to best structure contracts for these efforts.

IT Capital Planning/Enterprise Architecture: In many public sector organizations, budget formulation is managed through some form of Capital Planning and Investment Control (CPIC). Generally, CPIC manages the IT Investment Management process (development of business cases) and submits proposed IT budgets for submission to The Office of Management and Budget (OMB) for the agency via Finance. Oftentimes, there is analysis done in partnership with an Enterprise Architecture and Governance organization(s) around recommended IT investments and portfolio alignment for the budget submission. Both of these personas generally should be engaged at the business level and have a clear understanding of what the business needs and wants and how to translate that into IT and Budget terms. These two types of personas allow for expertise crossing budgeting, contracts, and IT which is needed in gaining buy-in across the organization and being able to translate across other personas involved in cloud FinOps.

Contracting Officer Representative (COR)/Program Manager: A COR savvy in IT and contracting that has a pulse on the workings of the Cloud effort is key.Many times, the subject matter experts (SMEs) working on the Cloud Initiatives rely heavily on a knowledgeable COR that understands their IT requirements and contracting needs. Many public sector organizations will have to invest in the training of CORs to fulfill this role. Additionally, many public sector organizations pair a Federal COR with a PM from the CSP to support this function.

Program Manager: In many organizations, the COR may also be a program or project manager involved in the cloud initiative(s). Many public sector organizations will have to invest in the training of PMs to fulfill this role. Additionally, many public sector organizations pair a Federal COR with a PM from the CSP to support this function.

Cyber Security: a Cyber Security Persona may be concerned with tracking compliance and security from an ATO perspective. IT Security is usually aligned with Enterprise Architecture and weighs on IT Portfolio alignment during the budget formulation process. This persona is cognizant of adherence to cyber security best practices and how they may differ in the cloud. Memorializing your agency's approach to these will be important.

Cloud Services Provider (CSP): a Cloud Services Provider is responsible for the services they provide the agency. When selecting services from your cloud provider, being aware what portions you are responsible for versus the cloud provider is important. However, in the public sector, there will often be at least one other persona between you and the CSP via a reseller.

Cloud Managed Service Provider (CMSP): A Cloud Managed Service Provider is responsible for services on top of what the CSP providers for its services. For example, with Infrastructure as a Service (IaaS), the CSP is typically responsible for everything at the infrastructure level. The organization is then responsible for the running of the applications, maintenance of operating systems, etc. An organization may choose to use a CMSP to do some of this work. In those instances, it is important to have a clear cut RACI defined for the responsibilities across all personas.

Reseller: Different Resellers may have different restrictions and access controls for obtaining console or detailed billing. When selecting a reseller or a contract, consider the level of detail and access available to you for enabling FinOps. In already existing contracts and Reseller agreements, put pressure on them to provide the level of detail or access needed for FinOps if they are not already providing it or not providing within a timely manner.

Stage 2

Socializing FinOps for adoption in an organization

You've done your research, you have your plan, and you know who to engage. The use of Cloud itself, and the adoption of FinOps represents a large-scale change to the way that IT is procured and used, and the way that organizations receive value from IT investments. It turns many existing procurement, financial management and engineering processes on their heads. This is why socialization of the key concepts behind FinOps is so important. Using the information gathered in stage 1, conversations with your stakeholders can begin.

- Communicate the values that are central to the change at all relevant levels of the organization (from executives to project teams) and share how FinOps adoption will benefit their teams.
- Share a short summary of what you "see" the future organization to look like
- Share a high-level roadmap

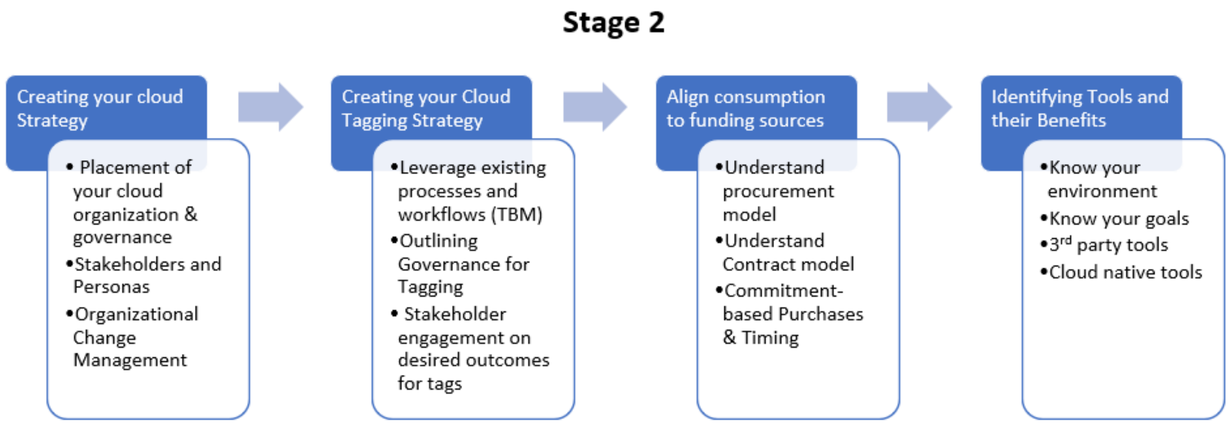
Create FinOps conversations with identified impacted teams, such as Finance lead(s), product lead(s) and lead engineer(s) to:

- Provide an understanding of what FinOps is. Offer to conduct "lunch and learns" describing FinOps to all organizations who may be participating in your FinOps initiatives
- Understand their issues and explain/educate on how FinOps could help them

- Discuss proposed KPIs and adjust per conversation feedback
- Establish interaction model between FinOps and key partners (IT domains; Controllers; App Teams)
- Identify future members during socialization for CCoE and Executive SteerCo.
- Customize the FinOps Model (Inform, Optimize and Operate) for the organization
- Identify the FinOps team with internal transfers where there is overlap with existing roles or individuals; fill remaining gaps via recruiting / contracting
- If FinOps capabilities don't exist in-house, then look to contract out. Determine where in the organization this role will sit. (CCOE, existing PMO, Policy Planning staff, TBM office, etc.)
- Socialization is part of organizational change management
- Map the change network for FinOps across the organization - sponsors, influencers, adopters. Create a clear training and communications strategy that stakeholders sign off on which ensures full coverage of all impacted resources
- If the organization is huge to reduce dependency on the central team, one scaling approach is to create a hub-and-spoke change management roll-out model
- KPI Roadmap: Finalize first-set of KPIs and reports, and identify and plan for next-gen KPIs and reports
- Document all of these items for your agency's FinOps playbook

Defining the Initial FinOps Model

In defining your initial FinOps model, there are many components to take into consideration. These components range from your overall Cloud Strategy, Cloud Tagging Strategy, organizational change management, and tool selection.


Stage 2
Creating your cloud Strategy
• Placement of your cloud organization & governance
•Stakeholders and Personas
•Organizational Change Management
Creating your Cloud Tagging Strategy
•Leverage existing processes and workflows (TBM)
•Outlining Governance for Tagging
• Stakeholder engagement on desired outcomes for tags
Align consumption to funding sources
•Understand procurement model
•Understand Contract model
•Commitment-based Purchases & Timing
Identifying Tools and their Benefits
•Know your environment
•Know your goals
•3rd party tools
•Cloud native tools

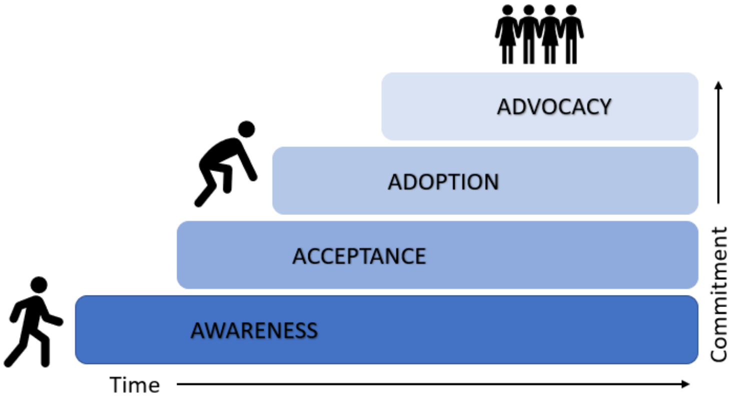
Creating your Cloud Strategy

There are numerous ways to create your cloud strategy and organization, some of which is very much a part of the stage 1 above. Whether you create or align to a Cloud Center of Excellence (CCoE) or another form of governance and organization already existing, it is important to address cloud (and FinOps) specifically within your organization. Cloud deviates from a traditional model in many ways (simply look at this playbook!) and involves a clear vision and communication to implement within your organization. Whatever path you choose for your Cloud Strategy (tailored to your agency), we want to call out some of the considerations we feel are important to incorporate as part of your strategy.

Organizational Change Management

Change management and tagging are both organizational and cultural changes. Wherever possible, try to leverage existing processes in order to streamline efficiency and minimize change in an operation. However, where changes to the processes are necessary, ensure those changes are backed by education and knowledge of why a process is being changed and the benefits and impacts of that change.

It is also critical to have a roadmap of your immediate, short-term, and long-term goals pertaining to cloud and tagging strategies so that your change management processes can plan and grow with those strategies.



Understanding the change management processes can help determine what sort of tagging may be needed to support change requests within the environment. It should also be fleshed out as a part of your overall governance and organizational strategy for cloud. Ensuring that tagging is a part of the creation of the resource is an important process that should be built into any change management workflow and can save time and money in the future by having this developed.

Automation

Consistent with the FinOps Crawl, Walk, Run approach, automation can be a helpful and critical component of tagging and resource creation/decommission. Depending on the type of environment or timeline, may be something that is set up in the overall tagging strategy but not immediately implemented. Just about any environment can benefit from even a small amount of automation. Taking the time to flesh out automation as part of the overall cloud strategy, outlining goals and KPIs for automation, and having consistent top-down guidance on automation standards and best-practices will result in an abundance of benefits both short and long-term.

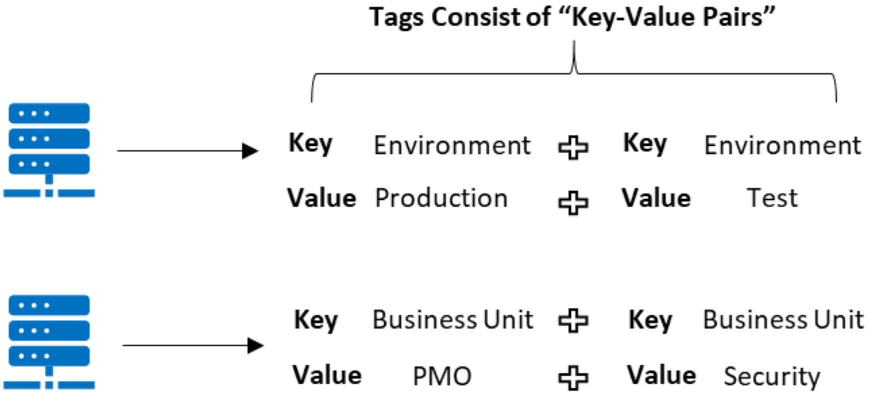
It can be easy to get caught up in the ways to optimize and rightsize. After all, this is a key benefit of utilizing the cloud. However, it is important to understand the impacts of the actions taken to rightsize and optimize. By developing automation or spending time rightsizing, many benefits in cost and operations efficiencies can be realized, but those benefits may lessen over time. Understanding the costs in developing these capabilities will allow you to calculate your savings efforts against the cost to optimize. Conducting business and technical case analysis for these capabilities and the savings should be done with the stakeholders outlined in the Personas section. These are also considerations to include in vendor comparisons for managed services and capability pricing.

Creating your Tagging Strategy

A FinOps model should consider an overall tagging strategy which accounts for the cloud services and resources that will be deployed, the functions that workloads are supporting, and the way in which cost & operational needs should be distinguished.

Additionally, consider leveraging already existing taxonomy or processes from your TBM implementation. TBM and FinOps go hand-in-hand and any strategy should seek to leverage the strengths of TBM and FinOps into one working solution. Taking insights from Stage 1 - Planning for FinOps, use the knowledge of your planned environment to flesh out the tagging taxonomy and strategy.

Include governance and processes for implementing the tags, and consider all resources (containers, serverless, non-taggable items) when coming up with a plan of execution.



For example, an environment running entirely on standalone VMs and storage may have a different tagging strategy than one that is a mix of containers, serverless, and other cloud services.

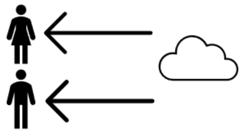
Similarly, a finance team who wants to capture cost by Application, function, or contract line item number (CLIN) might have a different tagging strategy and taxonomy to support those efforts than one who wishes to capture costs by project, team, or environment. With tagging, the potential to capture data in a variety of ways is near limitless and as such it is important to have a clear idea of the end goal of the tags to guard against unnecessary or "nice-to-have" tagging, especially in the crawl/walk phase.

Ensure a clear workflow and RACI are defined for who owns the tags, resources, and application of the tags as this will streamline efficiencies and assign responsibilities for maintaining tagging standards within your environments. For additional guidance on developing a tagging strategy, see the Cloud Tagging Strategy Guide developed by the DCCOI PMO in collaboration with the Cloud & Infrastructure CoP's Cloud Working Group. This guide can be found on CIO.gov.

Aligning Consumption to Funding Sources (Showback and Chargeback)

Showback is the ability to show charges by product or department, keeping expenses in a centralized budget. This can only be accomplished with a robust tagging strategy discussed earlier. If resources, workloads, accounts, subscriptions etc., are not tagged or labeled appropriately, any showback or chargeback report will have increasing variance.

Chargeback is the ability to take the charges of each department or chosen entity (such as application or system) and send those expenses to the entity for billing.



While showback and chargeback are both integral parts of FinOps, they can potentially take on a different role within the public sector. Some cloud contracts may roll up to one or two line items, in which case showback/chargeback is not necessarily needed for the purposes of the contract. However, because there may be many initiatives, programs, or divisions utilizing the same contract, showback and chargeback become a way to distinguish internally what each of your cloud areas are doing and how they are performing within the cloud.

This can especially become key in budgeting and forecasting exercises. Many divisions and sub-agencies may be leveraging the same cloud contract, but their need to track their own budgets and spend are critical in this scenario to ensure that in over/under burn scenarios funding is applied back to the correct division. As an example, this can be accomplished by organizing your cloud contract programmatically by CLIN and funding lines of accounting, whereby each program can account and track for specific obligations accordingly at the CLIN level and make adjustments, if required, at the level.

Commitment-based Purchases & Timing

Reserved Instances, spot instances, savings plans, etc can be a great way to capitalize on cost optimization opportunities, however it is important to work with the finance, contracts, and procurement stakeholders to ensure 1) timing for purchases 2) restrictions on purchases based on contractual limitations (if any).

A commitment-based purchase typically allows for discounted prices in exchange for your commitment to use either a minimum level of resources or spend a minimum amount, for a specified term of one or three years. Most government contracts will not allow for the purchase of a 3 year commitment, as such, knowing what your contract allows and implementing preventative procurement controls for items which can’t be purchased is key for effective use of commitment-based purchases.

As with 3 year commitment restrictions, there may be other restrictions around the use of 1 year commitments. Some might not allow 1 year commitments either, or only allow the purchase to occur at certain times (such as at the beginning or end of a contract period). It is key to understand if your contract will allow you to utilize commitments and if there are any restrictions on when they can be used. If your agency has taken a multi-cloud approach then understanding how commitment-based discounting works is crucial.   Just as important is the ability to merge those plans so there’s a holistic view of each vendor's commitments.

As with any procurement model, ensure to incorporate a process to track and manage commitment-based purchases, whether it is through a tool or another form. Have discussions around how to amortize these procurements or reflect them in any dashboards for stakeholders.

Identifying Tools and their Benefits

In Stage 1, Planning for FinOps in an Organization, we highlighted knowing your environment and its data classification. With this groundwork and the additional considerations below, identifying potential tools and their benefits for your environment will be easy.

Cloud spend & consumption data can be a cumbersome and confusing endeavor in any organization. Cloud spend data typically is received in files which contain anywhere between hundreds of lines for a small environment to millions of lines in larger environments on a monthly basis. While Cloud invoices are rolled up line items that normally can't provide much insight into your cloud spend outside of what you owe.

However, cloud spend & consumption data, while intimidating in its size and complexity, is available in near-real time and can be leveraged to make dynamic changes within your environment and see the results instantly instead of waiting for an invoice to confirm there were positive (or negative) results from the changes you made.

With this potential, the ability to process this data into meaningful insights and actionable items is a key component of why utilizing a tool can be beneficial to understanding your cloud environment and its costs and cost drivers.

The amount of tools in the market can be overwhelming. The process for narrowing down your options can begin with your organization's decision to use one or multiple cloud service providers. Some tools are only available for specific cloud service providers and others support single or multi-cloud approaches.

Once your selection has been narrowed down to tools available for your Cloud Service Provider, further considering tools which have a FedRAMP accreditation may be the next step depending on your environment's classification of billing data. Work with your Cyber Security Team and/or Authorizing Official to determine your environment's need for an accredited tool.

With your selection narrowed, below are some considerations when deciding on a 3rd party tool to support FinOps in your organization.

Cloud Tool Considerations

Capability	Considerations a Tool which Provides	Example Use Case
Spend Transparency	● Ability to create multi-persona dashboards with additional drill-down and customization abilities ● Dashboards and reporting functions which allow for levels of actionable intelligence and information to all personas who may need access.	Each persona may have their own needs in a dashboard showing consumption and costs. Allowing customization via multi-personas can assist in ensuring each persona gets the information they need. A finance persona may need costs by CLIN but a program manager may need costs by service offering or project.
Tagging	● Provides tagging policies supported by your CSP(s) ● Automation of tagging where possible. Note: CSPs have their own tagging rules and formats which may not be consistent across other platforms. In a multi-cloud environment, having a tool to combine and ingest data from multiple sources can become key	An organization might have 3 types of tags which they wish to apply: Business, Operations, and Security. By having a tool which supports multiple CSP policies, a holistic view across multiple environments becomes possible.
Showback & Chargeback	● Allows views for showback and chargeback in dashboards ● Manual/automated allocation of costs to consuming units	Knowing if your organization will need showback or chargeback can be a key component in a decision. Some organizations may not need chargeback, and will want to select a tool which allows for showback or vice versa.
Purchasing Best Practices	● A reservation planner to manage reservation purchases ● Recommends purchases across the cloud vendors, showing the predicted savings. ● Allows to define risk profile with configuring savings and utilization threshold	An organization leveraging Commitment Based Discounts will need to have a process to manage and amortize those purchases and a tool can assist.

Waste and Consumption management	● Recommends multiple right sizing to decrease the cloud spend by eliminating idle resources	Metrics such as CPU, memory, and storage utilization can be leveraged to support the decision
Spend forecasting	● Estimates the upcoming cloud spends with combining the historic usage data and the usage trends across organizations	This can be particularly helpful for organizations who need to forecast and create budgets using cloud spend or consumption

Cloud Native Application and Tool Considerations

Ensure that when looking at cloud native considerations, look at services in the appropriate regions that are available. For example, AWS has all its billing in its commercial region. Ensure with security stakeholders that billing data and cloud native tools would be able to be used in the commercial region if everything else is within a GovCloud region.

All changes to any environment should follow the established processes for Governance and security established within your CCoE or change management process.

As with 3rd party tools, ensuring your cloud native tools are included in architecture and vetted / approved by your Cyber Security team and/or Authorizing Officer should be a consideration when selecting a cloud native solution

Amazon Web Services Native Services

Cost Explorer	● Easy-to-use interface to visualize, understand, and manage the AWS costs and usage over time ● Forecasts by predicting the usage of services over the forecast time-period for the services and resources selected, based on the past usage	FedRAMP not required*
Cost and Usage Report	● Contains the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, Reserved Instances, and Savings Plans ● Usages are itemized at account or organization level by product code, usage type, and operation. It can be further organized by Cost Allocation tags and Cost Categories with hourly, daily, or monthly levels of granularity	FedRAMP not required*
Amazon CloudWatch	● Monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources ● Provides up to 1-second visibility of metrics and logs data, 15 months of data retention (metrics), and the ability to perform calculations on the metrics stored	FedRAMP High (GovCloud) DoD IL4, IL5, and IL6

CloudTrail	● Enables governance, compliance, operational auditing, and risk auditing for AWS accounts ● Simplifies security analysis, resource change tracking, and troubleshooting. In addition, CloudTrail detects unusual activity in AWS accounts	FedRAMP High (GovCloud) DoD IL4, IL5, and IL6
Trusted Advisor	● Provides recommendations that help to follow AWS best practices. Trusted Advisor evaluates the user account through checks ● Provides users recommendation to optimize services and resources accordingly	FedRAMP High (GovCloud) DoD IL4, IL5, and IL6
Service Catalog	● Allows organizations to create and manage catalogs of IT services that are approved for use on AWS (such as restricting 3YR Reserved Instances but allowing certain 1YR Reserved Instances) ● Defines and manage applications and their metadata, to keep track of cost, performance, security, compliance, and operational status at the application level	FedRAMP High (GovCloud) DoD IL4 and IL5

Organizations	● Helps to programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows and simplify billing by using a single payment method for all your accounts ● Integrates with other AWS services to define configurations, security mechanisms, audit requirements, and resource sharing across accounts in the organization	FedRAMP High (GovCloud) DoD IL4 and IL5

**Customers are able to leverage this service by agency approval*

Azure Native Services		
Azure Cost Management & Billing	● Tracks resource usage and manage cloud costs across all clouds with a single, unified view, while accessing rich operational and financial insights ● Implements governance policies for effective enterprise cloud cost management and increase accountability with cost allocation and chargebacks	FedRAMP High DoD IL2, IL4,and IL5
Azure Advisor	● Analyzes the configurations and usage telemetry and offers personalized, actionable recommendations to help optimize Azure resources for reliability, security, operational excellence, performance, and cost ● Configures Advisor to target specific subscriptions and resource groups, to focus on critical optimizations	FedRAMP High DoD IL2, IL4, IL5, and IL6

**Customers are able to leverage this service by agency approval*

Google Cloud Native Services

Reports and Dashboards	● Utilizes the billing report to view and analyze Google Cloud usage costs using selectable settings and filters. It also shows the forecasted usages and cost trends ● Visualizes and understand the effectiveness and financial impact of the committed use discounts (CUDs) purchased using CUD analysis reports ● Creates custom billing reports based on exported billing data (such as usage, cost estimates, and pricing data)	Check with AO for suitability
Budgets, Alerts, and Quotas	● Set threshold rules to trigger email alert notifications and use Pub/Sub for programmatic notifications (for example, to forward your budget messages to other mediums or to automate cost management tasks) ● Configure rate quotas (to limit the number of requests made to an API or service) and allocation quotas (to restrict the use of resources that don't have a rate of usage, such as the number of VMs used per project at a given time) to prevent unforeseen spikes in usage and overloaded services	Check with AO for suitability
Recommender	● Helps admins optimize Google Cloud resources by making proactive, actionable recommendations with a data-driven machine learning approach ● Recommender that can be executed with a few clicks helps optimize the cloud for price, performance, and security, thus maximizing the ROI	Check with AO for suitability

**Customers are able to leverage this service by agency approval*

Note: Cloud Service Providers are constantly adding exciting features and tools to their offerings to support these similar capabilities, while this list has some current ones to consider for government regions as a starting point, reference your cloud service providers services or reach out to your service provider for more information on what is available to you.

Forecasting and Budgeting for Cloud

Stay Tuned!

Forecasting and budgeting has challenges and hurdles no matter what industry or sector you are in. However, we recognize forecasting and budgeting can be a huge hurdle in the public sector for cloud (we've experienced it, too!). As such, stay tuned for a speciality play from us on using FinOps to forecast and budget your cloud spend at any stage in your cloud journey.

Acquisition of Cloud

Stay Tuned!

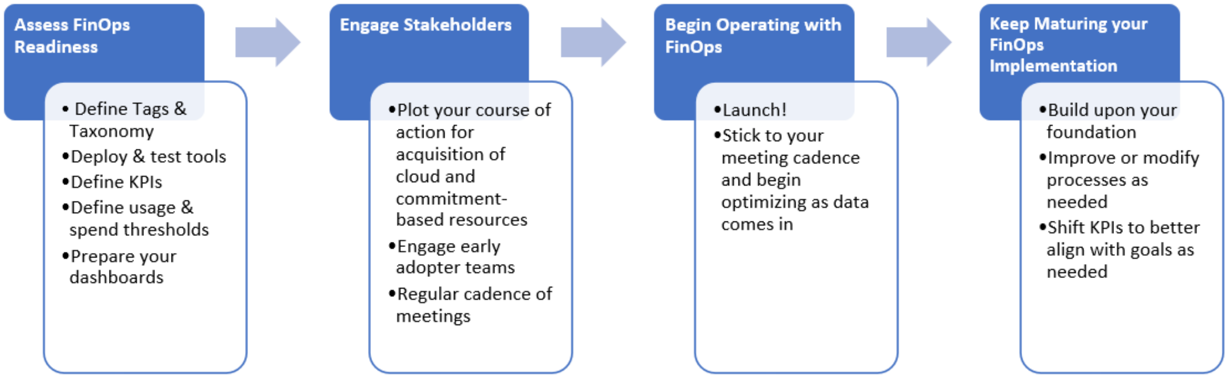
Similar to forecasting and budgeting, acquisition of cloud within the public sector is an interesting challenge due to the nature of cloud being outside of the traditional CapEx model. Stay tuned for a specialty play from us on acquisition of cloud to help you with your journey!

Stage 3

Preparing the organization for FinOps

In the previous two stages you have engaged stakeholders, aligned your cloud strategy and tagging strategy with your cloud goals, selected a tool or tools to assist in your cloud journey, and worked through various processes and workflows. In Stage 3, you will define your taxonomy, measurements of success, and begin implementing your processes and workflows. All of this should occur with continued communication with your stakeholders and personas.

Stage 3



Assess FinOps Readiness

- Define Tags & Taxonomy
- Deploy & test tools
- Define KPIs
- Define usage & spend thresholds
- Prepare your dashboards

Engage Stakeholders

- Plot your course of action for acquisition of cloud and commitment-based resources
- Engage early adopter teams
- Regular cadence of meetings

Begin Operating with FinOps

- Launch!
- Stick to your meeting cadence and begin optimizing as data comes in

Keep Maturing your FinOps Implementation

- Build upon your foundation
- Improve or modify processes as needed
- Shift KPIs to better align with goals as needed

Assess FinOps Readiness

- Define tags, metadata, and organizational taxonomy. With consideration to CLIN/SLIN, security, change management, and operations.
- Deploy, configure, and smoke-test tool(s)
- Finalize the first wave of KPIs. KPI's/Business adoption metrics can evolve over 'adoption periods' to create a 'crawl, walk, run' mentality and not push full maturity in one go. This will allow for less mature teams and executives to not be 'scared off' and do it step by step.
- Define usage and spend thresholds for alerts and report limits
  With consideration that adding funding may take a greater length of time, and so thresholds and alerts should be proportionate to when procurement needs to be notified
- Define and prepare persona-based self-service dashboards.
  These should show important metrics like the first wave of KPIs, cost allocation, budget anomalies, optimization recommendations, and other views of interest to stakeholders

- Prepare a forecasting model with unit cost calculations included. At this point, this is likely just a spreadsheet.

A final assessment with your stakeholders should occur at the end of this stage to determine the readiness for the organization to launch its FinOps operation from conception into reality.

Engage Stakeholders

- Determine business unit appetite for commitment levels (total cost for enterprise discount negotiations, commitment-based discounts, marketplace, and professional services) aligned with your contract vehicle.
- Engage early adopter teams to get optimization wins (e.g. shutting down test environments or instances which are no longer in use to show material savings). These are important for socializing, rolling out, and winning additional adoption later
- Get some additional early governance wins for getting FinOps implemented (e.g. tagging policy, lease-to-live automation, etc.)
- Start cadence of regular meetings. The FinOps/CCOE team should be talking on a regular basis with the business units, app teams, practitioners and stakeholders to implement best practices and track KPIs.

Remember that if the organization has multiple business units operating from a federated cloud operating model they will have differing levels of maturity. It is important that the change management considers this and allows them to adapt at differing paces.

Begin Operating with FinOps

With your groundwork laid out, processes and strategies established, and stakeholders engaged and on-board, your FinOps organization is ready to launch. Ensure that your processes and principles are incorporated into meetings and metrics. Spend time reviewing at a regular cadence the goals and status of your FinOps rollout. Ensure stakeholders remain engaged and that as personnel are on-boarded into your organization they are brought up to speed on your agency's FinOps initiatives.

Keep Maturing your FinOps Implementation

Assess your maturity as you crawl, walk, and run in your FinOps journey. It is our hope that you use this playbook as a launch-point for that journey. However, be prepared to continue to work and re-work as your organization grows and matures. By having a strong cloud governance and organization strategy in place, you'll have all of the foundations needed to succeed even when changing your individual FinOps processes. We also encourage the utilization of other resources such as other agencies implementing FinOps. For additional resources and training on FinOps please refer to the FinOps Foundation.

Acknowledgements

The FinOps Foundation extends a huge thank you to the members of the US Government Working Group that broke ground on this documentation, including members:

- Melvin Brown II, Office of Personnel Management
- Amanda Dalton, Deloitte Consulting
- Florence Kasule, US Digital Service
- Tim Siegel, PBG Consulting
- Tim Cooke, ASI
- Daniel York, General Services Administration

- Ylanda Hill, Department of Housing and Urban Development
- Bill Nieusma, CirrusLabs
- Christian MacMillan, Office of Management and Budget
- Chris Gomba, Office of Management and Budget
- Jamal Rittenberry, Office of Management and Budget
- Sina Farahani, Deloitte Consulting
- Thomas Santucci, General Services Administration