

# Federal Cloud Strategy Guide

*Agency Best Practices for Cloud Migration*

The Data Center and Cloud Optimization Initiative Program Management Office (DCCOI PMO)

General Services Administration  
Office of Government-wide Policy



## Acknowledgements

This document would not have been possible without the help of an interagency working group, including contributors from General Services Administration, the National Institute of Standards and Technology, the Department of Energy, the United States Air Force, the National Aeronautics and Space Administration, the Department of Justice, the U.S. Army Corps of Engineers, the Federal Aviation Administration, and many other individual contributors.

## Table of Contents

<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>3</b>
<b>Stakeholder Analysis</b>	<b>4</b>
<b>Assumptions and Constraints</b>	<b>7</b>
<b>Current State Assessment</b>	<b>8</b>
<b>Strategy Sections</b>	<b>11</b>
Business Value	11
Risks	13
Procurement/Acquisition	14
Workforce	20
Compliance & Security	31
Target State Environment	37
Automation	44
Governance	48
Finance	57
Exit Strategy	62
<b>Appendix I: References</b>	<b>67</b>
Cloud Computing Definition	67
<b>Appendix II: Best Practices</b>	<b>69</b>
Procurement Resources	70
Workforce Resources	70
Compliance & Security Resources	77
Governance Resources	80

# Executive Summary

## Strategy Timeline

Agency cloud strategies are meant to be living documents, allowing for constant refinement in response to changing factors, such as economic and technical conditions. This strategy guide should be used alongside Organizational Change Management (OCM) best practices to continuously evaluate agency-specific goals, objectives, and initiatives. Using this method ensures alignment to mission and performance needs. Key management approaches should:

- translate governing policy, requirements, and standards;
- facilitate communication and collaborate across the agency and stakeholders;
- establish guidelines and responsibilities;
- identify opportunities to evolve and modernize; and
- promote efficiency through strategic partnerships across their agency.

## Introduction

This document will assist you with developing an agency-specific strategy for successful cloud adoption. This document covers the major topics to consider in your cloud strategy. Cloud strategies should fit the agency-specific mission, business, technology, and security needs. There is no one-size-fits-all approach for cloud adoption and its subcomponents of planning, migration, and operations.<sup>1</sup>

For purposes of this guidance document, the term “cloud” is most accurately applied to those solutions that exhibit the five essential characteristics of cloud computing, as defined by NIST SP 800-145: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.<sup>2</sup>

Agency cloud strategies require a responsive planning and management framework, meaning you should continually reassess your strategic approach to cloud adoption. OCM best practices will help you manage and sustain the change needed for operations to efficiently achieve the full value of cloud and reduce the risk of implementation setbacks due to workforce resistance. Many of the steps outlined in this document mirror those for application rationalization,<sup>3</sup> which provides agencies with effective processes to maintain and enhance their IT portfolios. As you begin to regularly survey your application

---

<sup>1</sup> Additional reference materials: Cloud Smart, President’s Management Agenda, Application Rationalization Playbook

<sup>2</sup> See Appendix I, “Cloud Computing Definition” for additional information from NIST Special Publication 800-145

<sup>3</sup> The Application Rationalization Playbook: An Agency Guide to Portfolio Management. CIO Council. <https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf>

ecosystem, you create a feedback cycle that informs and shapes cloud strategy development.

We encourage you to share best practices and lessons learned from your own cloud adoption efforts. As new opportunities and challenges arise with cloud technology, this document will be updated with new information to assist you in refining agency-specific cloud strategies.

We also encourage your agency to use this document as a guide to develop a comprehensive cloud strategy that supports your business and mission objectives. There are many methods associated with strategic planning and you may already have a model to follow. Whatever model you choose, it's important to include long-term, medium-term, and short-term activities to shape your goals, objectives, and actions. Together, these form the basis for your Enterprise Cloud strategy.

A comprehensive plan also identifies milestones and timeframes associated with the actions in the plan. The following notional list of goals and objectives provides an example of how to structure your strategic plan.

### **Goal 1: Build the foundation for your agency enterprise cloud capability**

- Objective 1.1: *Establish a comprehensive suite of cloud capabilities and processes that serve all agency cloud business and IT needs*
- Action 1.0: *Establish contract for cloud acquisitions*

### **Goal 2: Transform your IT workforce**

- Objective 2.1: *Strengthen the current workforce to enable staff members to better use cloud technologies to deliver services*
- Action 1.0: *Provide vendor training classes to agency workforce*

Once you have developed your goals, objectives and actions, you can easily develop an overall roadmap with timelines on how to proceed. This document provides best practices and recommendations that will serve as input to your planning process.

## **Stakeholder Analysis**

Successful cloud strategies and activities require vertical and horizontal alignment within the organization, from top leadership to operational staff. You first need to identify the relevant agency stakeholders and determine what their interests, goals, and perspectives are in relation to the cloud. OCM best practices for communications and stakeholder engagement will help you increase collaboration and stakeholder buy-in. While an open

source search will yield several different frameworks, you should create and follow a framework that best suits your agency-specific needs. You are encouraged to conduct an initial analysis in your planning phase and then reassess during both implementation and Operations and Maintenance (O&M) phases to account for changes in stakeholder roles and responsibilities. The following is a high-level overview of the recommended stakeholder analysis for agencies.

### Stakeholder Analysis Steps

1. **Identify key stakeholders.** People that will be affected by cloud services, have influence or power over cloud services, or have a vested interest in the adoption of cloud services.
2. **Identify customers.** People, groups, or institutions that will be served by any cloud adoption.
3. **Classify providers.** Entities, including vendors or other agencies, who will provide the cloud services. Be sure to include the mechanism that governs the relationship with these providers (written contract, IAA, working group, etc.).
4. **Recognize leadership.** Individuals within your agency that must approve any cloud-related items, especially related to overall strategy. This group includes those with statutory authority for decision making and informal champions you can leverage to assist with your cloud projects.
5. **Analyze implementers.** People tasked to implement the cloud strategy and provide support for all phases of your cloud projects.
6. **Group and prioritize stakeholders.** A prioritization and categorization of stakeholders to help navigate where and how in the process your agency will engage each stakeholder.

**Sample Agency Stakeholders**

<b>Internal IT Group</b>	<b>Internal Supporting Organizations</b>	<b>External</b>
IT Operations	Procurement	OMB
Plans and Programs	Finance/Budgeting	Congress
Enterprise Architecture	Human Resources	The Public/Press
IT Security	Application Business Owners	Vendors

When identifying stakeholders, you should not only identify specific roles, but also have an updated list of individuals for each position. The list keeps your cloud team organized and able to effectively communicate in the event of staffing changes within your agency.

After completing the brainstorming session, categorize the identified stakeholders in terms of influence, interest, and levels of participation in your cloud migration efforts. Figure 1 shows a common stakeholder analysis technique, the power-interest grid, which was originally published by Colin Eden and Fran Ackermann in their book “Making Strategy,” a power-interest grid<sup>4</sup> to map stakeholders.

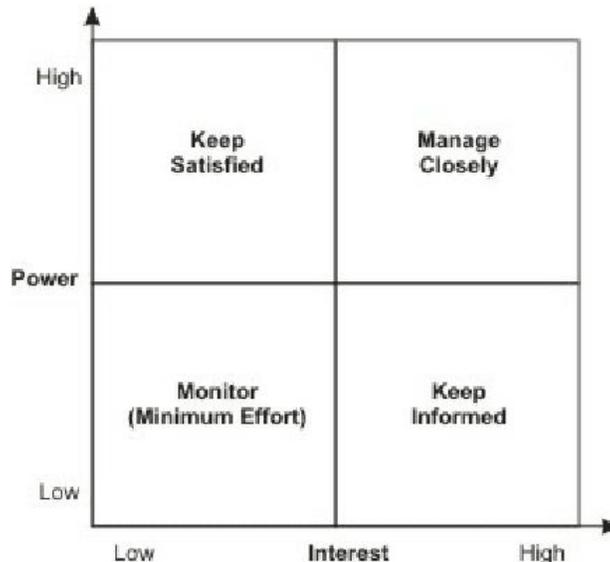


Figure 1. Power-interest grid

1. **High power, high interest:** These stakeholders need to be managed closely and should be fully engaged in your cloud projects. Close communication and serious consideration of needs and feedback from these stakeholders is a priority.
2. **High power, low interest:** These stakeholders are important because of their influence within your agency but may not be as interested in cloud projects as others. A lower level of engagement and communication should be utilized, while addressing any concerns to ensure they remain satisfied. Over communicate to this group.
3. **Low power, high interest:** These stakeholders are interested in your cloud projects, but may have less influence across your agency. Keep these individuals adequately informed of your cloud efforts and leverage their expertise for specific tasks where appropriate.

---

<sup>4</sup>“Making Strategy” by Colin Eden and Fran Ackermann

4. **Low power, low interest:** These individuals should be the lowest priority when factoring in feedback and needs of various stakeholders and require limited communication to ensure they are adequately informed.

For a strong cloud strategy, we recommend developing a communications strategy to address each type of stakeholder. Communications strategies should include information about how each stakeholder group will react to the final strategy. This exercise prepares you to manage stakeholders and navigate roadblocks. Below are a series of questions to consider when brainstorming stakeholder reactions:

- Beyond cloud, what are the primary interests each stakeholder has towards the agency and to each other?
- What are the key impacts (political, reputational, technical, financial, etc.) of a cloud strategy for each stakeholder? Which stakeholders will experience financial consequences?
- What is each stakeholder's current disposition towards cloud? If they are in favor of cloud adoption, what do stakeholders want to achieve with the cloud? If they are opposed, what is driving the resistance to the cloud?
- What type of information is needed from each stakeholder to successfully create a cloud strategy and should that information be shared with each stakeholder?
- Are there connections between stakeholders and what are the relevant sources of influence?

Once you complete your stakeholder analysis, take the time to develop a communications plan. This plan should guide how each stakeholder will be informed on all cloud strategy related matters, including ways to overcome opposition, resolve disputes, and create buy-in.

## Assumptions and Constraints

Clearly articulate the assumptions and constraints in the cloud strategy to set expectations within your agency. While the cloud provides many positive opportunities to agencies, the assumptions and constraints may impact the benefits the cloud can offer (cost, schedule, performance). Identify assumptions and constraints early in the process to develop effective contingency plans and avoid major obstacles. You should review and determine your own agency-specific assumptions and constraints. Examples of assumptions and constraints are:

- Misconceptions about cloud services<sup>5</sup>
- Regulatory and statutory requirements
- Resource allocation
- Human capital
- Business cycles
- Legacy platforms or architectures
- Governance, risk, or compliance
- Budget and time
- Lack of provider skills and expertise
- Legal and compliance limitations
- Contractual limitations
- Process limitations
- Procurement of cloud services
- Critical agency mission dates
- Expiration of existing contracts
- Technology refresh cycles
- Hardware at End of Life/Support
- License/Software maintenance renewal dates
- Agency workforce capabilities vs. needed training/contract support

## Current State Assessment

Evaluate people (functions, roles, capabilities), processes (frameworks, reviews, procedures/guidelines), and technology (databases, solutions, tools) across the agency. Understanding the interdependencies and strengths of your current environment helps the cloud strategy team innovate, and/or maximize agency effort. Complete an agency-specific cloud readiness assessment and ensure you have proper documentation for enterprise architecture and other processes.

During your assessment, consider specific circumstances and the scope of planned cloud projects to determine which steps should be completed before developing your cloud strategy. Having accurate information about your agency's IT ecosystem helps you identify the most impactful and cost effective cloud projects. This assessment process may also uncover processes within your agency that can be improved. Consider materials, such as your agency's Federal Information Technology Acquisition Reform Act (FITARA) and Federal Information Security Management Act (FISMA) scores, to create an accurate picture of your agency's IT ecosystem. Resolving any challenges or priorities highlighted within your FITARA and FISMA scores helps simplify and improve cloud adoption efforts.

Not all steps are necessary for launching a simple cloud pilot project. Steps one, two, four, five, and six are the core items that must be completed. Steps three and seven are helpful

---

<sup>5</sup> <https://cloudserviceevaluation.com/>

but not an absolute requirement. Agencies are encouraged to complete all of the steps for a more substantial cloud migration or adoption initiative.

### **Suggested Steps and Activities Needed to Assess Current State<sup>6</sup>**

1. Inventory current IT assets
  - List servers (including VMs) and their OS, plus any middleware components
  - List facilities where infrastructure is housed
  - List data connections for each infrastructure grouping and their capacity/utilization
  - List application interfaces and all dependent systems
  - Search, discover, and identify “Shadow IT”
2. Inventory and assess current applications and data
  - List names of stakeholders for each application, including owners, system administrators, and end users
  - Document current physical location of host and bandwidth availability/utilization
  - List OS, storage, processing, database, libraries requirements
  - Document network bandwidth requirements for each application over time, including connection type (e.g., VPN)
  - Ensure there is an ATO for each application covering FISMA/FIPS PUB 199 impact level and security needs and access controls and dependencies (e.g., Microsoft Active Directory, Method of Authentication, and SSO)
  - Define the life expectancy of the application
  - Identify the Level of Effort (LOE) and skill set needed to maintain the application (admins, programmers)
  - Document the points of integration between the application and other systems
  - Define email services, such as Simple Mail Transfer Protocol (SMTP) servers for receiving outbound emails generated by the application
  - List network and systems monitoring tools used by your agency’s Network Operations Center, including those for cyber security and performance
  - List messaging queues such as an Enterprise Service Bus (ESBs) or other middleware
  - Understand what other internal and external applications depend on data furnished by the application being migrated, documenting the routing and IP address
  - Create a data governance plan. A sound plan includes assessing which data is fit for the cloud

---

<sup>6</sup> “Table 5. Suggested Steps and Activities Needed to Assess As-Is State,” DoD Cloud Computing Acquisition Guidebook, DAU, December 2018.

- Analyze applications that will be moved into the cloud to determine if any need to be refactored, modernized, upgraded, and/or certified to run in a cloud
    - NOTE: There is no one size that fits all solutions. Remember that not all applications should be moved to the Cloud.
3. Inventory current software licensing and maintenance agreements
    - Ensure your organization has a software manager, per OMB M-16-12, that is responsible for managing, through policy and procedure, all agency-wide commercial and COTS software agreements and licenses. Understand the details regarding licenses as some Cloud Service Providers (CSPs) write their agreements where they require a license per vCPU
    - List software licensing model (e.g., seats, servers, clients) for all applications, including cost and length of term
    - Document and review your open source software, adhering to OMB M-16-21 requirements
  4. Document current network
    - Ensure network architecture is documented and understood, especially connection points and boundary management
    - Determine whether there is sufficient connectivity, bandwidth, and redundancy to support cloud services. An organization may have to make network upgrades to acquire commercial cloud services.
    - Document Access Control Lists (ACLs)
  5. Review existing IT governance
    - Review current configuration management policy documentation covering provision and allocation of current compute resources across your agency's departments
  6. Plan for change management
    - Review your existing change management strategy. Having a strong governance model is key to successfully migrate to the cloud. If the organization has solid IT Service Management (ITSM) processes in place for Asset Management, Configuration Management, and Change Management, then this activity will be much easier to manage.
  7. Review existing workforce capabilities
    - Identify the current cloud skill capabilities of your existing workforce and factor in the differing needs of various cloud service models
    - Consider workforce capabilities when completing your application inventory and identify the specific skills required for each

## Conclusion

While these steps will help you understand the current state of your agency, funding and workforce limitations make this step challenging to complete. Waiting to complete the assessment process may delay your cloud migration and adoption efforts. It's important to consider the specific needs of your agency and weigh the decisions that need to be made

before beginning a cloud strategy initiative. You can use other factors, such as your agency's FITARA and FISMA scores, to determine the risks and benefits of moving forward with a cloud project before you complete the entire assessment process (depending on your agency and the type of cloud projects you plan to execute). A smaller cloud project with limited scope may be a useful starting point for your agency, and taking lessons learned from this effort may help you complete other steps within the assessment process. There is no one-size-fits-all approach for every agency. This document intends to help inform and assist you in developing your own unique strategies for cloud migration and adoption.

## Strategy Sections

### 1. Business Value

Formulating a business case and calculating a Total Cost of Ownership (TCO) estimate for cloud adoption is the first step in developing your cloud strategic plan. It's imperative to understand what value your agency gains from investing time and resources for cloud adoption. Capturing the business value helps stakeholders understand, accept, and commit to cloud investment and migration activities. Conducting a crosscutting analysis of your agency's existing environment enables the cloud strategy team to identify opportunities and needs for the future state.

Achieving cloud efficiencies is challenging and you need to take a holistic approach. Prioritize cloud services for new IT service acquisitions and create a business case that supports the adoption of the technology. Identify what business challenges you are trying to solve — (e.g., increasing cost savings, scalability or accessibility) prior to migration. This is key to conveying why the change is needed. As you assemble your business case, identify the benefits you expect to receive after deployment.

#### **Business Case Considerations:**<sup>7</sup>

- **Agility:** The ability to make capacity available more quickly.
- **Scalability:** Increasing your global footprint and the ability to increase and scale capacity.
- **Data center efficiency and optimization initiatives:** Efforts to reduce your data center footprint and use cloud resources to support those workloads. Agencies should review the Cloud Smart policy<sup>8</sup>, which offers practical implementation guidance for agencies to fully achieve the full potential of cloud-based technologies.<sup>9</sup>

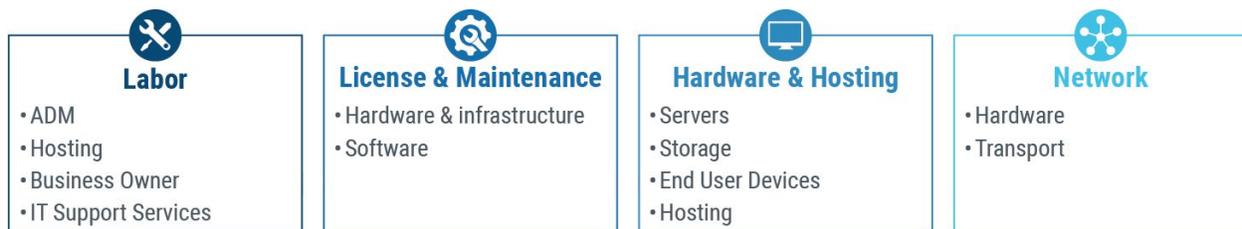
---

<sup>7</sup> "Designing A Cloud Strategy Document," Gartner. January 5, 2017.

<sup>8</sup> <https://cloud.cio.gov/strategy/>

<sup>9</sup> <https://cloud.cio.gov/strategy/>

- **Cost transparency:** Better visibility into expenses because cloud usage is metered. Review different contract types to understand their levels of transparency and determine what works best for your agency.
- **Moving from Capital Expense (CAPEX) to Operating Expense (OPEX):** Shifting from a traditional procurement model of capital expenses to an operational expense model where resources are metered and paid for as they are consumed.
- **Availability:** Cloud providers can achieve and deliver availability in regions and through architectures that many traditional enterprise organizations cannot economically achieve.
- **Customer satisfaction:** Downstream customer experience improves greatly with increased agility, scalability, and availability.
- **Total cost of ownership (TCO):** Calculate and capture the full range of maintenance costs for each application, beyond DME and Operations and Maintenance (O&M). Agencies can also consider their TBM efforts when making these financial decisions. Figure 2 shows an example approach.



**Figure 2. Sample TCO Calculation Approach<sup>10</sup>**

Use this model to calculate TCO and include other considerations when developing your business case. For example, procurement costs, FITARA- and FISMA-mandated requirements and reporting, service management costs, among other areas can be factored into this process.

### **Define Success Criteria in Business Case<sup>11</sup>**

Creating a successful cloud strategy requires your agency to define and articulate success metrics. Without these, it's difficult to assess when cloud migrations are complete and difficult to prove they are successful. A common milestone to determine if migration was successful is when the O&M organization assumes complete control for the cloud environment, including the transfer for all engineering documentation and administrative accounts. Some examples of completion and success metrics are:

- Successful proof of concept for a specific application or workload
- Developed cloud provider functionality criteria
- Security considerations
- Cost targets met and any variances from expectations are understood

<sup>10</sup> <https://www.ciosummits.com/BusinessCaseForCloud.pdf>

<sup>11</sup> "Designing A Cloud Strategy Document," Gartner. January 5, 2017.

- Performance characteristics align to baseline expectations
- Contractual and service-level agreement (SLA) requirements met
- Service quality requirements meet end-user requirements (uptime and incident resolution)
- Data protection and availability plan defined and tested (backup and disaster recovery)
- Established exit strategy
- Regulatory requirements understood and addressed
- Mission value (mission achievement, cost efficiency, increased agility, access to modern capabilities, innovations, etc.)
- Acquire data to develop success criteria and metrics

## 2. Risks

Identifying and mitigating risks is standard practice for any successful cloud strategy, and this document does not prescribe a specific framework to adopt. Open-source research yields several different risk models and vendors frequently provide risk analysis as part of their contract support. If your agency decides to follow a pre-constructed framework, you should adapt it to your agency's specific circumstances. You should approach developing a risk framework by grouping risks into salient categories. For example, risk can be categorized into three areas: mission, business, and people; or cost, schedule, and performance. To be clear, these are suggested groupings and you should feel free to go in different directions. Simply starting with a foundation sets you on the right path. Below are some examples of types of risk you should account for in developing a risk strategy:

- Changing from owning to on-demand funding models
- Workforce skills
- Security risks
- Specific risks to organization
- Maintaining legacy systems
- Variable cloud costs
- Disruptions to customers during cloud adoption
- Changing legal and compliance regimes
- Cloud Outages by Cloud Provider or Agency Shared Service Provider

To further illustrate how to assess risk, a sample framework from the Program Management Institute (PMI) is provided below.<sup>12</sup> PMI offers several risk frameworks but the one below explains how to identify and rank risks. PMI instructs users to answer the following questions to help flush out risks at the start of any project:

- What can vary positively or negatively more than 5% from what is expected?

---

<sup>12</sup> See PMI's Capturing Project Risk Produce Results Control. <https://www.pmi.org/learning/library/capturing-project-risk-produce-results-control-8266>.

- What surprises have we encountered in the past on this type of project?
- What can go wrong?
- What else can this cause to go wrong?
- What can go extremely well?
- What else can then go extremely well?
- What do we not know?
- What do we not know we do not know?

Once you identify risks, develop a way to assess them to appropriately prioritize which to address and how. Like risk frameworks, there are several ways to perform risk assessments but the common challenge for any approach lies with identifying and quantifying the degree of each risk. The MITRE Corporation offers four best practices for developing risk assessments<sup>13</sup>:

1. Tailor the assessment criteria to the the decision or project;
2. Document the rationale for the assessment of impact and probability;
3. Recognize the role of systems engineering; and
4. Tailor the prioritization approach to the decision or project.

Treat the process of developing a risk assessment as a fact-finding mission and ask a series of questions to flush out what exactly you are trying to assess. Some examples are:

- Are there weaknesses in the security architecture that can be exploited by hostile actors?
- What are the potential business impacts of an unmitigated risk?
- What hostile actors would attempt to take advantage of any risks?

After moving through the risk identification and assessment steps, consider what type of mitigation plan needs to be developed. It's impossible to mitigate every aspect of an identified risk so keep that in mind when budgeting time to develop your mitigation plan.

### 3. Procurement/Acquisition

Once the current-state assessment is complete and you have considered the business value and risks of cloud adoption, consider how to procure and acquire cloud services. Cloud procurement follows the same format as the regular procurement process but can have some added complications. Review your existing IT contracts, available shared government services, and available government-provided cloud service providers. This streamlines or eliminates most steps from the procurement and acquisition process. Early engagement with government subject-matter experts (SMEs) and review of government

---

<sup>13</sup> See MITRE's Risk Impact Assessment and Prioritization: <https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization>

resources - especially the use of RFI's - helps frame the project and the solicitation so goals are met. As part of your market research, you should review technical research on the technology and capabilities available in the commercial market, as well as acquisition research to determine the best acquisition mechanism to procure what cloud services you need. GSA's [Cloud Information Center](#) has a number of valuable resources for cloud procurement.

The following 11 areas require close collaboration between agency program, CIO, CTO, security personnel (ISSO), general counsel, inspector general, and privacy and procurement offices to acquire cloud computing services:<sup>14</sup>

1. **Review your data:** Identify the data and information you want to move to the cloud, including its classification (compute, store, transport).<sup>15</sup>
2. **Select a cloud:** Choosing the appropriate mix of cloud service and deployment models to meet your agency requirements and mission.
3. **CSP and end-user agreements:** Fully integrate Terms of Service and all CSP/customer agreements into cloud contracts.
4. **Service-level agreements (SLAs):** Define performance with clear terms and definitions to demonstrate how performance is measured and what enforcement mechanisms are in place. Many CSPs have standard SLAs, so make sure you review and understand the terms.
5. **CSP, agency, and integrator roles and responsibilities:** Carefully delineate the responsibilities and relationships between agency, integrators, and the CSP.
6. **Standards:** Use the NIST cloud reference architecture as a guide to ensure the agency and CSPs use the same terms and definitions for cloud services.
7. **Security:** Carefully detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment.
8. **Privacy:** If cloud services host "privacy data," take time to identify potential privacy risks and responsibilities and address these needs in the contract according to the appropriate requirements.<sup>16</sup>
9. **E-discovery:** All data stored in a CSP environment must be secure and available for legal discovery (e.g., able to be located, preserved, collected, processed, reviewed, and produced).
10. **Freedom of Information Act (FOIA):** All data stored in a CSP environment must be available for appropriate handling under the FOIA.
11. **E-records:** CSP's must understand and assist with Federal Records Act (FRA) compliance and obligations under this law.

---

<sup>14</sup> Creating Effective Cloud Computing Contracts for the Federal Government  
<http://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/cloudbestpractices.pdf>

<sup>15</sup> Review FIPS 199 policy <https://csrc.nist.gov/publications/detail/fips/199/final>

<sup>16</sup> Agencies should consider requirements for the specific type of data, including but not limited to Federal Information Processing Standards (FIPS), FedRAMP, DOD Impact Levels, FITARA, HIPAA, Personally identifiable information (PII), Records Management, etc.

## Cloud Contract Basics

There are several contract types used to acquire cloud services available to agencies: firm-fixed-price (FFP), labor-hour, incentive, cost reimbursement, and time and materials (T&M). Each of these contract types have their own benefits and challenges, which you should carefully consider before making a decision. Using a FFP contract may make the most sense in some circumstances but the risk is loss of flexibility and cost savings that are capable with contract's that aren't fixed price. A contract only for labor-hours may also be an appealing option, but because the cloud services themselves are not included, a second acquisition action is required to acquire the cloud services unless using services from another government agency via an Interagency Agreement (IAA). Consider an incentive contract when FFP isn't appropriate and the required supplies or services are cheaper. An incentive contract ties the amount of profit or fee payable under the contract to the contractor's performance. T&M contracts are difficult because FAR defines cloud services as a "material," which makes them unappealing to vendors due to profit restrictions. However, a T&M contract may be useful to migrate a custom application tool into the cloud where labor may make up most of the cost of the contract. It's important to consider these factors (and those detailed later in this section) to determine the cloud procurement and acquisition model that suits your needs.

You may struggle to procure and execute cloud services contracts due to workforce challenges or limited resources if you work at a smaller agency or agency component. If you're unable to fully complete the current state assessment discussed earlier, you should at least determine the unique applications and tools your agency uses or which commercial products best suit your environment. Agencies may find commercial tools and applications are less labor-intensive products to migrate into the cloud. An agency component may benefit from leveraging existing cloud expertise of its parent agency for its cloud efforts. If your agency continues to struggle to contract cloud services, you can consider current cloud shared services options, review existing acquisition vehicles, blanket purchase agreements, assisted acquisition services, and government cloud service providers.<sup>17</sup>

## Cloud Payment Models

There are numerous pricing models for commercial cloud services available to the Federal Government, but agencies face different funding and contracting constraints than those faced in private industry. For example, agencies cannot incur obligations in excess of contract funding<sup>18</sup>, cannot front-load funding for cloud services more than reasonably expected<sup>19</sup>, and may face difficulties in situations where unexpected demand factors, such as disasters, exist. If an agency deems a T&M contract too risky, agencies are already

---

<sup>17</sup> <https://cic.gsa.gov/acquisitions/acquisition-resources/>

<sup>18</sup> Anti-Deficiency Act information and requirements  
<https://www.gao.gov/legal/appropriations-law-decisions/resources>

<sup>19</sup> Review bona fide needs rule requirements. 31 USC § 1502

innovating to utilize flexibilities available to them that currently exist in the FAR. Agencies use four approaches to pay for cloud computing services today, including:

- Approach 1: Optional CLIN Not to Exceed (NTE)
- Approach 2: Drawdown Accounts
- Approach 3: Subscription Based
- Approach 4: Blended Model

Approaches 1 and 2 rely on creating a per unit of sale FFP contract and monitoring the burn rate to control cloud services and labor costs in a similar approach to a traditional T&M contract. When negotiating these contracts, agencies should focus on the cloud capabilities sought, and not prioritize specific hardware that may become obsolete over time. Agencies need to have a contract management governance policy in place to monitor costs. Cloud Service Providers generally provide cost management tools that will allow agencies to forecast and monitor costs and to establish cost/budget thresholds warnings. In addition, agencies should include terms on how to take advantage of price reductions over time as the vendor's price for cloud services declines. These cost savings can be built into the contract or negotiated on a regular basis with the vendor. Approach 3 sees a CSP providing a bundle of cloud services at a fixed monthly price for a defined period of time using a subscription method. Agencies would still obtain the benefits of these cloud services, but may not achieve substantial cost savings, as they are paying for services that may not be fully utilized.

#### **Approach 1: Optional CLIN Not to Exceed (NTE)**

- The cloud contract contains one or more optional contract line item numbers (CLINs) for cloud hosting services, and the agency obligates money to a CLIN as needed. The contract may have one CLIN tied to an incremental funding clause with a capped ceiling value on the CLIN to control costs.
- Benefit: This is the most common method for funding the cloud and is the traditional method of contracting for IT services.
- Challenge: The agency is unable to easily ramp services up based on usage, but may be able to ramp down to decrease the burn rate. If there is significantly higher utilization than originally planned for when estimating funding for the CLIN, there may be a need to exercise an option to surge that specific CLIN capacity and increase costs. As a result, there may not be a full realization of the benefits of elasticity of cloud in terms of cost savings.

#### **Approach 2: Drawdown Accounts**

- Government monitors model: The agency engages with a vendor and agrees to a contract for several years of 12 month periods of performance. For example, an agency may agree to terms with the vendor such as \$50 million over 5 years, which comes to \$10 million per year. The agency obligates the initial \$10 million annual amount, with the vendor providing a monthly bill for services and the agency draws down from the account with the obligated funding to pay the vendor. The agency

continues to monitor the burn rate and requests additional funding if the account funds get low.

- Vendor monitors model: The vendor receives a lump sum from the agency to pay for cloud services and draws down against the account. The vendor monitors the burn rate and notifies the agency once funding falls below a certain amount, as well as provides an estimate as to how long the remaining funds may last. The agency then provides additional funds to the account as needed to maintain services.
- Benefits: Allows agency customers to realize elasticity and flexibility benefits of the cloud.
- Challenges: Burdensome for agency and vendor to track funding as cloud usage can be unpredictable.

### **Approach 3: Subscription Based**

- Subscription model: The vendors bundle a fixed amount of cloud services to the agency for a recurring charge each month. The agency determines its needs and costs upfront, and obligates funding for the time period, which is usually one year.
- Benefits: This model works well if cloud services are consistent through the life of the contract. There is low risk, certainty of utilization, and simple contract execution.
- Challenges: The agency may seek a higher level of cloud services than forecasted to create a buffer if unexpected circumstances arose, resulting in the risk of paying for services that are never fully utilized. This nullifies the cost flexibility benefits that cloud services provide by only paying for services that are used.

### **Approach 4: Blended Model**

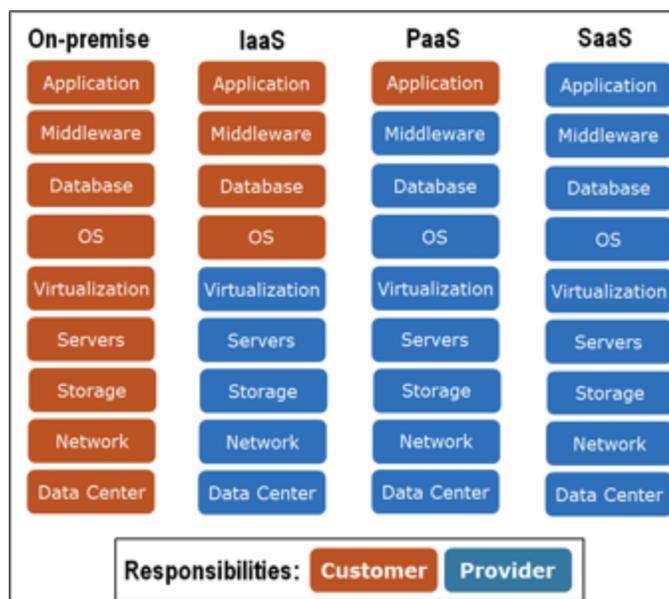
- Hybrid model: An agency determines its utilization rate using historical data center and cloud data. The agency uses a subscription based model to meet most of its utilization needs (ex. 80%), and then uses other models to meet its remaining needs to manage demand fluctuations.
- Benefit: Provides flexibility and benefits from each of the different models.
- Challenges: Using model cloud payment models requires increased planning and management.

These methods of buying cloud services are minor variants in the existing contracting structure, and may not effectively address the problem of demand elasticity and portability. None of these methods provide a complete realization of the benefits of cloud services by providing effective means for an agency to both consume and pay only for the resources it uses and needs. A potential solution would be to explicitly allow for cloud service resource units to be treated like labor hour rates (fixed unit price) in T&M contracts.

### **Cloud Service Models**

There are three service models as defined by NIST: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model, shown in

Figure 3, has different characteristics and subcategories from the consumer standpoint and requires different approaches to management and payment conditions.



**Figure 3. Primary Service Models<sup>20</sup>**

Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) share characteristics such as application hosting replacements for traditional servers housed in an agency’s data center. In a subscription based model, a fixed amount of computing services is bundled together and the agency is charged monthly. One major consideration for both IaaS and PaaS models is whether or not IT professional services are needed in support of the service model. For agencies procuring IaaS and PaaS without professional services, a FFP contract can be used. Contract risks should be relatively low and predictable within acceptable limits, however agencies should consider lack of cost transparency and that they can be charged for services not used or are charged more than expected. In cases where agencies require support services, a hybrid contract type should be considered that includes a FFP CLIN for the IaaS and PaaS, and a Labor Hour CLIN for the support services. Aside from the CLIN types, agencies should ensure the CLINs are scoped appropriately but broadly to provide flexibility (e.g., labor, services, travel).

SaaS offerings differ in that vendors typically charge for active users or seat licenses that are permitted to access the service. SaaS seats may be scaled up or down each month, or other appropriate time period, to keep with the metered billing model in a T&M or FFP contract. Use a T&M contract to pay for usage and take advantage of the SaaS cost savings. Automation tools help provision, control access, and provide cloud monitoring and reporting. If you select a FFP contract type for a SaaS procurement, allow for flexibility at

<sup>20</sup> Acquiring Cloud presentation, DAU

the CLIN or TO level so cost savings can be realized. Table 1 outlines what to consider to successfully align a service model with the ideal contract type.

**Table 1. Service Model Aligned to Contract Type Considerations<sup>21</sup>**

Service Model(s)	FFP Considerations	T&M Considerations
Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS)	<ul style="list-style-type: none"> <li>• Use when no professional services needed</li> <li>• Use when vendor and agency agree on price</li> </ul>	<ul style="list-style-type: none"> <li>• Use when support services required (should be separate from FFP order)</li> <li>• Identify support needs in CLINs</li> </ul>
Software as a Service (SaaS)	<ul style="list-style-type: none"> <li>• May be favored by agency CO</li> <li>• Needs to allow for flexibility at CLIN or TO level to enable savings</li> <li>• Limit to seat-oriented contracts</li> </ul>	<ul style="list-style-type: none"> <li>• Usually used for SaaS</li> <li>• Enables better cost savings</li> <li>• May be difficult to obtain CO buy-in</li> </ul>

### Legal and Contractual Clauses

There are a number of important legal and contractual clauses an agency must consider when selecting and acquiring a cloud service. Agencies can refer to the joint CIO Council and CAO Council guidance document, “Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service,” to review best practices and lessons learned on cloud services acquisitions.<sup>22</sup> This document should be your agency’s first resource on legal and contractual topics such as:

- CSP and end user agreements
- Service level agreements
- Privacy
- E-discovery
- FOIA access
- Federal recordkeeping
- Law enforcement, Inspector General, cyber incidents

## 4. Workforce

Careful consideration of your workforce is key to the success or failure of any cloud initiative. You need to ensure your existing workforce has the skills, knowledge, and abilities needed to successfully adopt cloud platforms, move applications to the cloud, or

<sup>21</sup> Acquisition Professional’s C.A.S.T.L.E. Guide.

<https://fcw.com/-/media/gig/fcwnow/documents/2017/castle-guide-v11.0-20170830.pdf>

<sup>22</sup> “Creating Effective Cloud Computing Contracts for the Federal Government.” February 2012.

<https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf>

purchase commercial cloud services. If you move too quickly to modernize technology and neglect workforce modernization, your team will struggle to effectively utilize their new cloud environments. The result is more resources are spent training or recruiting new talent, which delays and reduces the expected benefits of the cloud. It is important to correctly identify the skills needed (by position) to support the new cloud environment.<sup>23</sup> This section guides you in identifying the critical workforce skills needed and proposes several ways to fill those gaps during cloud strategy development.

In June 2020, Federal Chief Information Officers Council released a report that analyzed the major challenges affecting the Federal IT workforce.<sup>24</sup> This update – the Future of the Federal IT Workforce – is a follow-up to the State of Federal Information Technology Report released in 2017, which provided an overview of the current and future state of federal IT. Agencies should review this document as a resource when assessing and developing their cloud workforce strategy.

Successful workforce development requires coordination across the C-suite. CIOs should work closely with CHCOs for all areas related to IT professionals at your agency. Determine the responsibilities and roles for different teams across your agency to ensure your hiring and recruiting teams have a clear understanding of the technical skills required for your IT staff.

You must define a human capital management approach to successfully engage leadership, correctly leverage existing staff capabilities, and attract and retain top talent.<sup>25</sup> Review the following factors and tools to better understand your agency’s workforce capabilities and needs and guide the development of your approach:

- Conduct a Workforce Analysis
- Training and Skill Development
- Recruiting and Hiring Talent
- Matrixed Organizational Teams and Contract Support
- Structural and Cultural Change (managing resistance)

While hiring is one possibility, there are also many alternative ways to address gaps, including: reskilling existing employees via internal or external training programs; short and long term contractor positions; automation; outsourcing non-classified processes; and

---

<sup>23</sup> For an example of the roles and skills for a cloud team, see Cloud Dream Team Member List in the Appendix Section.

<sup>24</sup> <https://www.cio.gov/CIO-Council-Releases-the-Future-of-the-Federal-IT-Workforce-Update/>

<sup>25</sup> “Change Management in the Federal Workforce, Accelerating the Gears of Transformation.” December 2019.

<https://www.opm.gov/policy-data-oversight/workforce-restructuring/reshaping/accelerating-the-gears-of-transformation/guidance-for-change-management-in-the-federal-workforce.pdf>

matrixed team models. The Chief Human Capital Officers Council (CHCOC) Reskilling Toolkit is a good guide to develop a path for reskilling in the cloud space.<sup>26</sup>

### **Workforce Mapping and Skills Gap Analysis**

Your first step in reviewing your workforce capabilities is to determine what skills are needed for the specific cloud services your agency will be adopting. You also need to identify existing human capital to meet your agency's Cloud Strategy goals, which includes identifying the specific skill sets and certifications needed for roles and levels or teams. This process should be completed by team leads or individuals familiar with the current and desired state of your agency. Create percentage estimates for the breakdown between entry-, mid-, and senior-level employees as well as an overall total number of employees. The following is key to shaping the end-state map<sup>27</sup>:

- Identify skills that help your agency achieve its mission, strategy, and goals.
- Identify the current and future skills staff need to have success in their roles. Think about these in terms of the different phases of your cloud projects.

Once you understand the future state of your workforce, you need to focus on the current state. This piece of the workforce map can be developed by a number of different groups, including team leads, a portion of the HR division, or even outside consultants. Complete skill assessments through employee surveys or interviews, skill management software, or performance reviews. You must consider the goals and motivations of employees to achieve and maintain high workplace satisfaction. The following questions are key to understanding your current-state workforce:

- What talent is available across your agency? Are employees flexible to move to new functions and roles?
- What employee development efforts are in place to maintain employee skills and develop competencies to address future agency challenges?
- What functions can be consolidated or performed through other mechanisms like contract support?
- What knowledge transfer efforts are in place to capture institutional knowledge?

In accordance with the Federal Cybersecurity Workforce Assessment Act of 2015<sup>28</sup>, agencies are encouraged to use the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework as a guide to identify all federal civilian positions

---

<sup>26</sup> To access the CHCOC's Reskilling Toolkit:

<https://www.opm.gov/policy-data-oversight/workforce-restructuring/reshaping/accelerating-the-gears-of-transformation/reskilling-toolkit.pdf>

<sup>27</sup> US Office of Personnel Management. Migration Planning guidance information documents: Workforce Planning Best Practices. October 7, 2011.

<https://www.opm.gov/services-for-agencies/hr-line-of-business/migration-planning-guidance/workforce-planning-best-practices.pdf>

<sup>28</sup> pages 735-737 at <https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>

performing IT or cybersecurity-related functions.<sup>29</sup> While the NICE Framework helps to standardize the skills you need, it's strongly recommended you build on it and perform enterprise-wide skills assessments to account for all necessary skills.

After you create your workforce map, focus on creating a strategy to address any skills gaps you identified. The type of skills needed to fully support the cloud environment will vary from agency to agency but below is a sampling of the skill types you should consider for new talent:

- Network Engineering
- Cloud Security Architecture
- Systems Administration for Vendor Specific Platforms
- Financial/Accounting Skills
- Portfolio/Program/Project Management (Cloud/IT Focused)

Your workforce analysis should also include the skills and resources needed at each stage of your cloud adoption and migration efforts. For example, you may initially need a great deal of technical expertise and support at the start of the process but you may not require as much support once you reach the operations and management phase. Consider the length of your projects and whether it makes sense to rely more on government or contractor staff for each stage of the project.

### **Training and Skill Development**

A highly engaged, motivated, and trained federal IT workforce must be able to stay up-to-date with the newest developments in technological tools and methods. Just as programming languages, networking paradigms, and storage media have all evolved over time, the skills required to manage these technologies have required updating as well.

Filling skill gaps by training current employees is just as important as recruiting new talent to your agency. Your existing workforce has considerable experience and understanding of your agency's mission and you should enable this intellectual capital and institutional knowledge, while ensuring employees are adaptive, flexible, and willing to learn new skills. Your workforce analysis may uncover a need for your agency to reskill and upskill existing staff. It may be necessary to reshape functions, processes, and procedures to align your workforce with current or anticipated requirements of your cloud strategy. Employee engagement is also a key driver to the program's success. Partner with Human Resources and agency leadership to actively address employee morale to improve workplace culture if needed.

You can develop native training or partner with other agencies or organizations to assist, like the Cloud Security Alliance and the Cybersecurity Education and Certification

---

<sup>29</sup> To access the NICE Framework: <https://csrc.nist.gov/publications/detail/sp/800-181/final>

Readiness Facility . There are several training frameworks you can use to improve your existing workforce:

- **Local:** Training classes for team members that need specialized training. The local model provides an environment separate from work, which reduces potential distractions.
- **In-House:** Best for agency-specific training. This model also allows for numerous staff members to be trained simultaneously. Partnerships with local training institutes are best for these because they generally use their own equipment, instructors, or materials.
- **Online:** Best for mass training and for a geographically dispersed workforce. The online model lends itself to partnerships with other organizations since it reduces the cost of providing training. You can acquire corporate licenses from groups to access specific training.
- **Hybrid:** Partner with colleges or continuing education institutions since these trainings require longer periods of instruction to cover very specific topics.
- **Vendor Specific:** These trainings provide insight into a vendor's particular product, but rarely go beyond the services and products offered by the same vendor. Most vendors are able to provide training to agencies, especially if such support is outlined in the Statement of Work (SOW). Cloud vendors often offer specific certifications for their products.

Regardless of the framework your agency chooses, you need to establish a training budget for immediate-, short-, and long-term training, education, and workforce development. Free training is available but detailed and technical trainings often incur costs for instructors, materials, or logistical support.

If the skill gaps you have identified within your agency are expansive and you want to leverage training, you must account for how to pay for the training as part of your workforce strategy. Consider partnering with other agencies to have larger training events. The benefit of partnerships is the ability to leverage the expertise of organizations that already have successful training programs and can potentially save you money. For example, inviting guest speakers and SMEs on specific topics from other federal agencies is another effective way to instruct and train your employees.

Once you've allotted sufficient resources and identified suitable reskilling candidates, design a reskilling program to prepare your IT workforce for the future. Increase the flexibility of IT workers' skills (both in breadth and depth) and empower reskilled workers to advance their careers beyond current time and grade restrictions. Establish curriculums and knowledge roadmaps that the workforce and management can use for career development tracks tailored to early, middle, and late career employees.

Agency leadership must embrace a workplace culture that values and promotes training opportunities for staff. Having supportive leadership encourages staff to take advantage of opportunities. One effective way to ensure your agency's IT professionals maintain skills is to set aside time on a regular basis for teams to complete individual training or take part in events as a team.

### **Workforce Metrics**

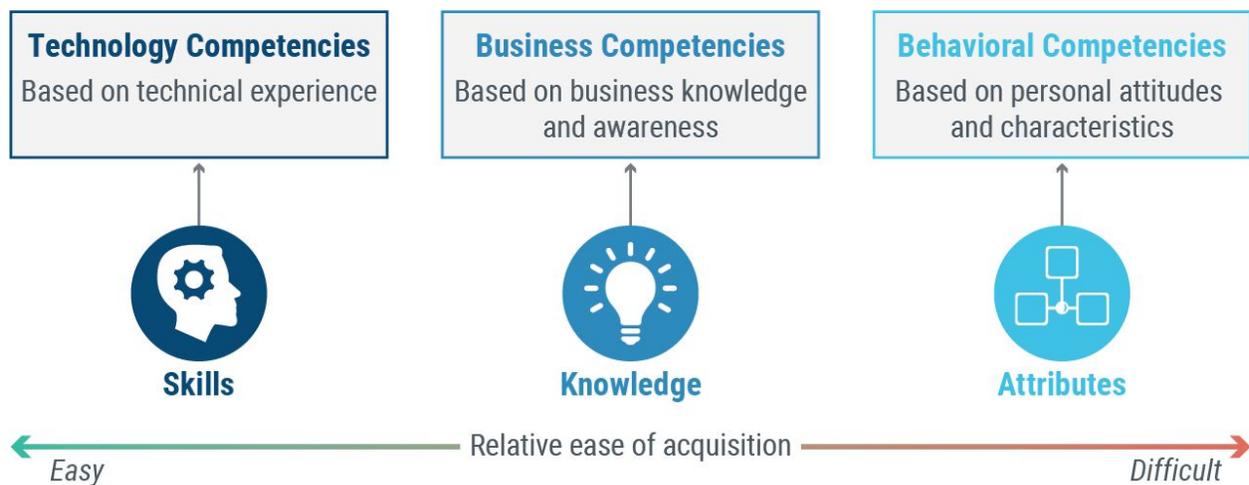
Metrics are critical to track the progress towards your workforce goals. Below are a few approaches to tracking employee capabilities:

- **Training Participation:** Often measured as a percentage of the potential versus actual attendees number of attendees at a training. This is not an indicator of knowledge retained but it does measure awareness of a topic, which is foundational for future skill development efforts. Types of training measured can include informal sessions, such as educational brown bags, as well as formal training such as conferences, webinars, seminars, etc.
- **Employee Readiness Assessment Results:** Tests actual knowledge retention or, in the case of new hires, incoming knowledge of the agency-identified skill sets. This can be measured in a number of ways, including by assigning a pass/fail classification or by using an A through F grading system for the completed assessment.
- **Adoption Rates:** One of the best indicators of effective change management, adoption rates are potentially a great litmus test for automation, especially in regards to cloud. The measurement of adoption is similar to training participation (e.g., the potential number of adopters versus those that have adopted the new system). This indicator has the potential to turn into a system of metrics that includes the measure of early adopters' percentage of adoption (e.g., determine whether the cloud is fully utilized or only used to complete specific tasks).
- **Certifications:** Measured as the count of the number and type of certifications within a certain agency, component, or bureau. It's important to note that, while certifications are an important aspect of training, they are not always a definite indicator of mastery on a topic.

### **Determine Who to Hire**

At this point, your completed Current-State assessment should have given you a sufficient understanding of the skills needed for your cloud migration efforts, as well as gaps. This analysis, coupled with the skills required for your agency-specific cloud efforts, inform which individuals and skill sets should be a priority for your agency to hire. For example, specific skill sets may be different for a SaaS, IaaS, or PaaS cloud project, because the level of agency vs. vendor management will vary. The more involved you are with management, the more your agency will need to have a workforce with adequate technical skills and knowledge. There may be some skill sets that are easier to develop through a few training

sessions, while others may take time and experience. The factors in Figure 4 should inform your hiring decisions.

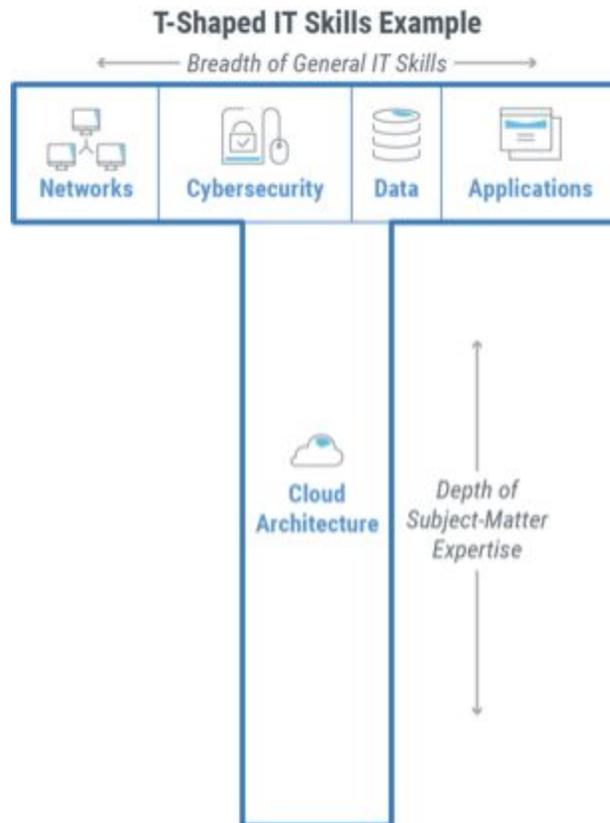


**Figure 4. Three Competency Types in IT Human Resources<sup>30</sup>**

The workforce of the future must not only adapt to the rapid pace of technological innovation, but also to the changing expectations about personal growth and career flexibility. Consider whether your future IT workforce should be built upon a “talent stack” in which IT professionals with a wider variety of talents and experiences would quickly adapt to new technologies and challenges. One way to achieve this flexibility is to adopt a “T-shaped” technological skills model (Figure 5), with depth in one discipline and breadth across multiple complementary skills. This concept has been used in the private sector as far back as 1991.<sup>31</sup> The T-shaped skills model enables future reskilling opportunities by building upon an increased breadth of experience.

<sup>30</sup> Application Leaders Must Deal With Hybrid Reality: Staffing and Skills for the Cloud-Based Application Organization. Gartner. July 14, 2016.

<sup>31</sup> “The T-Shaped Engineer.” American Society for Engineering Education. June 2015. <https://www.asee.org/public/conferences/56/papers/11576/download>



**Figure 5. The “T-shaped” technological skills model.**

To keep your workforce agile and modern, hire individuals with a broader set of general skills and then develop expertise as your agency’s cloud needs evolve. Not all federal IT professionals need to be an expert in every facet of cybersecurity. In the example provided in Figure 5 above, a cloud computing specialist might have a breadth of training in cloud-focused cybersecurity concerns, tools, and tactics.

### **Talent Recruitment**

Develop a comprehensive recruitment strategy if your agency’s cloud strategy needs direct hires. Consider whether an applicant has potential for long-term growth and success within your agency. Assessing a candidate’s “soft” and “hard” skills will help make that determination.

While the Federal Government typically cannot match the type of compensation offered by the private sector, there are still tactics agencies can employ to attract talent:

- **Geographic Diversity:** It’s difficult for many agencies to hire qualified IT professionals because the DC metro area has a large concentration of Federal IT jobs and a very competitive job market. Review opportunities to access the larger

IT-talent pool from across the country and recruit and hire the best job candidates from wherever they reside.

- **Mission:** Craft a narrative for prospective hires to highlight how their work can impact your agency's mission and improve overall service to the American people.
- **Incentives:** Agencies have a suite of incentives they can use for recruitment, such as relocation reimbursements, pay increases, or bonuses. You likely cannot leverage all types of incentives, but you can select the ones that attract the right type of candidate.
- **Source:** Explore the talent pool by using tools like LinkedIn, federal hiring events and posting positions on job sites (e.g., Monster).
- **Plain Language:** Use plain language for position descriptions to expand the audience for your agency. Many private-sector candidates are unfamiliar with how the Federal Government categorizes and describes particular skills, and may struggle with agency-specific vernacular and acronyms.
- **Include SMEs:** The more cross-collaboration, the stronger the talent will become. Technical SMEs need to be closely involved in the hiring process, beyond interviewing candidates. Per Office of Personnel Management (OPM) guidance, involve SMEs with job analyses, reviewing resumes and conducting structured interviews to screen out unsuitable applicants.<sup>32</sup>
- **Assessment Tools:** Use open-source assessment strategies or government resources to create assessment tools that determine if potential candidates can fill the appropriate vacancies.<sup>33</sup>

## Hiring Authorities

Once your agency workforce is mapped and existing skill gaps are identified, focus on how best to hire new talent. Encourage your agency to leverage special hiring authorities to quickly remedy the skill gaps because the complexities and average time-to-hire in the current federal recruiting process are much higher than the private sector. Below are some flexible approaches to consider.

- **Schedule A:**<sup>34</sup> Allows agencies to meet specific hiring needs that have not been addressed by using the regular competitive hiring process, with justification and OPM approval. OPM grants Schedule A hiring authority for digital services staff

---

<sup>32</sup> OPM. Improving Federal Hiring through the Use of Effective Assessment Strategies to Advance Mission Outcomes. September 13, 2019.

<https://www.chcoc.gov/content/improving-federal-hiring-through-use-effective-assessment-strategies-advance-mission>

<sup>33</sup> OPM. Assessment Decision Guide.

<https://www.opm.gov/policy-data-oversight/assessment-and-selection/reference-materials/assessmentdecisionguide.pdf>

<sup>34</sup> 5 CFR § 213.3101.

<https://www.govinfo.gov/content/pkg/CFR-2002-title5-vol1/pdf/CFR-2002-title5-vol1-sec213-3102.pdf>

working on IT projects for the past several fiscal years.<sup>35</sup> This authority is limited to agency staff working on IT Modernization, Smarter IT Delivery initiatives, and cloud migration projects.

- **Cybersecurity:** Released by OPM in October of 2018, this hiring flexibility is designed to meet critical technical and cybersecurity skill needs.<sup>36</sup> This guidance provides direct hire authorities for a variety of Scientific, Technical, Engineering and Mathematics (STEM) positions, as well as cybersecurity-related positions that have a severe shortage of candidates or critical hiring needs.
- **CIO:** In April 2019, OPM released its final regulation on *Delegation of Direct-Hire Appointing Authority for IT Positions*.<sup>37</sup> Building on the foundations of the PMA and Executive Order 13833,<sup>38</sup> this new CIO direct hire authority improves the Federal Government’s ability to recruit IT professionals by streamlining power into two distinct hiring authorities, one for a “severe-shortage of candidates” and one for “a critical hiring need.” Under this authority, appointments can last up to four years, with an additional four year appointment available at the agency’s discretion.
- **Schedule A(r):** For term appointments between one and four years.
- **Schedule A(u):** To hire employees with severe disabilities.
- **Direct Hiring Authority (DHA):** For specific roles. For example, GSA uses DHA to hire permanent IT Specialists for INFOSEC positions. You can contact your agency’s CHCO office and the CHCOC for more information, guidance, and support on various hiring authorities for IT professionals.<sup>39</sup>

### Communities of Practice and Rotation Programs

Knowledge sharing across government is key to ensure the Federal IT workforce continues to maintain and grow its skillset. One of the most effective ways to enhance knowledge and skill sharing is to build upon the existing success of interagency communities of practice (COPs). These groups bring together individuals that work in similar skill areas to share and discuss innovative work and best practices.

Another way to improve knowledge and skill sharing across the government is to expand existing rotation programs, which provide professional opportunities for federal workers at multiple agencies. Rotation programs, such as the Presidential Management Fellows<sup>40</sup> and

---

<sup>35</sup> OPM. Schedule A Hiring Authority for Information Technology (IT) Modernization and Smarter IT Delivery Initiatives. 11/17/2017.

<https://www.chcoc.gov/content/schedule-hiring-authority-information-technology-it-modernization-and-smarter-it-delivery>

<sup>36</sup> OPM. Announcing Government-wide Direct Hire Appointing Authorities. 10/11/2018.

<https://www.chcoc.gov/content/announcing-government-wide-direct-hire-appointing-authorities>

<sup>37</sup> OPM. Delegation of Direct-Hire Appointing Authority for IT Positions. 4/5/2019.

<https://www.chcoc.gov/content/delegation-direct-hire-appointing-authority-it-positions>

<sup>38</sup> Executive Order 13833. Enhancing the Effectiveness of Agency Chief Information Officers. 5/15/2018.

<https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers>

<sup>39</sup> For more information, visit: <https://www.chcoc.gov/>

<sup>40</sup> <https://www.pmf.gov/>

the Presidential Innovation Fellows,<sup>41</sup> appeal to those who are not interested in the standard career path available to employees at most agencies. Detail assignments and rotation programs increase retention and allow them to gain valuable new skills along the way.

### **Leveraging Matrixed Teams and Contract Support**

Matrixed team models enable you to maximize talent from across your agency. They foster greater opportunities for employee engagement at all levels and increase communication and the ability to efficiently source needed talent and skill sets across component boundaries. The result is an increased ability to optimize resources, mitigate cross-cutting risks, and influence agency-wide strategy.

You can also use contract support to fill skill gaps, either as the solution to identified gaps or a backstop while agencies hire FTEs with relevant skills. That said, it's important to clearly delineate the type of support vendors provide in the SOW. It's best practice to use federally accepted labor categories to target the types of skills needed, such as those provided by the NICE Framework. To avoid vendor lock-in, you should also include contractual language around knowledge transfer and post-contract support. Negotiate with vendors on providing extensive training support during and after the terms of the contract, when possible.

### **Fostering Structural and Cultural Change**

A culture that's ready and responsive to change is essential to both cloud strategy transformation and agency-wide success. Integrate change tactics into the broader framework of your transformational cloud efforts and continuously evaluate to ensure sustained progress. These tactics include: Strategy and Planning, Process Improvement, Business Integration, and Strategic Communications.

Create a change transition or transformation plan that conveys the case for change and engages stakeholder and workforce from across the agency. These plans, at a minimum, convey the implementation plan (e.g., workforce reskilling, training opportunities, hiring plans), communications (e.g., newsletters, all-hands, FAQ sessions), and stakeholder management (e.g., leadership buy-in and advocacy). Vertical and horizontal collaboration across the organization is critical to overcome resistance and these transition plans will promote both. Be sure to make plans available to all staff. For more guidance on how to tailor these plans, review the Federal Organizational Change Management Guide from the Federal Technology Investment Management Community of Practice (FTIM CoP).<sup>42</sup>

---

<sup>41</sup> <https://presidentialinnovationfellows.gov/>

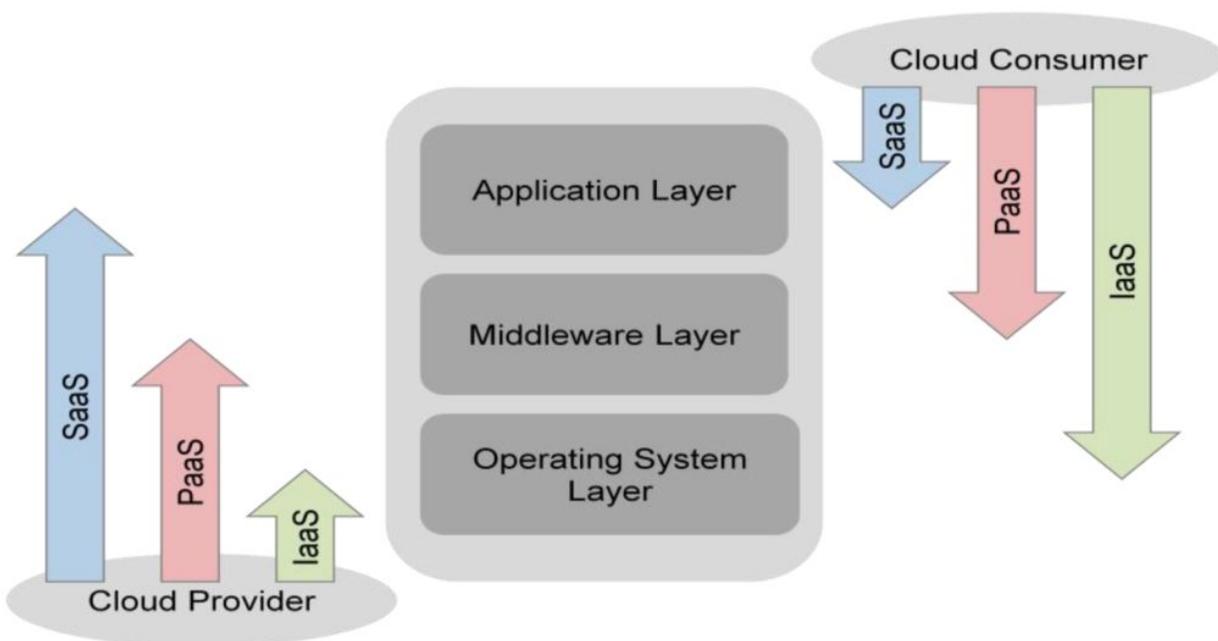
<sup>42</sup> Visit FTIM CoP's OMB MAX page to access the guide.

## 5. Compliance & Security

Improve your agency's ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

### Securely Transitioning to Cloud

Security concerns are inherent to cloud adoption during both the migration and ongoing risk management processes. Enterprises are increasingly at risk of unintentionally exposing data to the public internet and it's likely that cloud security failures will be the fault of the federal agency, not the cloud service provider (CSP). Managing these concerns helps keep security from hindering cloud adoption and keeps cloud adoption from hindering the mission of your agency. Since the CSP and customer both share control of resources, they also share security control (and liability for) of those resources. This is known as the Cloud Shared Responsibility Model (Figure 6), and varies by service model.



**Figure 6. Cloud Shared Responsibility Model<sup>43</sup>**

Just as in any other IT project, security must play a central role when creating your cloud strategy. From the onset of your cloud project, you need to factor in security considerations and your path to accreditation or Authority to Operate (ATO), including incorporating someone in your workforce with a knowledge of not only traditional ATO security considerations but also cloud-specific factors. In addition, your security considerations may be different if you are building a new system in the cloud or if you are transitioning an existing system into the cloud. If transitioning, pay careful attention to the existing security

<sup>43</sup> [https://www.nist.gov/system/files/documents/it/cloud/SP\\_500\\_293\\_volumell.pdf](https://www.nist.gov/system/files/documents/it/cloud/SP_500_293_volumell.pdf)

control implementation because the security control inheritance model changes and the cloud provider may (or may not) be providing this implementation. Highlight security controls that are not met in the current system to confirm that they are not overlooked in the cloud architecture even if they've been addressed through compensating controls. This becomes increasingly important as the security responsibility of the agency grows.

### **Implement Strong Identity Management Foundation**

Always consider the security implications of identities in the cloud. In cloud environments, identities act as a perimeter for protecting workloads and replacing network edge controls. When you adopt a specific cloud service, your agency should control access to data using cloud native access controls. These requirements are outlined in the ATO process but it's important to understand that it's the customer's responsibility to control access across all cloud service models.

Integrate cloud identities with existing identities managed by their current access management tool to create a single user pool. Although these controls would traditionally be role based, identity-based access control allows customized permission sets for each individual rather than placing users in overly-generous buckets. This is more complicated to manage than role-based access so your agency can rely on native or third-party, commercially available tools to help monitor privileges. Consolidating user directories helps you leverage the added security of custom permission sets. If possible, pilots should also utilize two-factor authentication, but this is not a requirement for a secure or successful pilot.

Multi-factor authentication is recommended to avoid the “domino effect” of a security breach gaining access to multiple accounts.<sup>44</sup> Federate identities to cloud data centers and enable single sign-on (SSO) to IaaS, PaaS and SaaS deployments either manually during the cloud deployment or through the service provider (many offer built-in SSO and identity management capabilities). While this granularity is more complicated to manage than role-based access, using native or 3<sup>rd</sup> party commercially available tools to assist in monitoring privileges and consolidating user directories can help your agency leverage the added security of custom permission sets. Regularly monitor access using these tools, particularly to flag when employee positions change. User Entity Behavior Analytics help catch anomalies and flag compromised user accounts. Cloud Access Security Brokers (CASBs) are one tool for monitoring activity and enforcing security policies, and can be either on-premise or cloud-based software. Maintain accounts by regularly “privilege trimming,” or removing unnecessary access, using these tools to automate the process.

Zero-trust security is a model for managing these access implications, not only between user accounts and data, but also between servers and applications. While traditional security models place a layer of security between agencies' internal assets and the external digital world, zero trust requires validation between any two endpoints. In a

---

<sup>44</sup> <https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication>

zero-trust model, one server requesting data from another would need to both be whitelisted by the server it's attempting to access and be able to present a certificate confirming that it's a trusted connection, thus validating the connection in two ways. In a cloud environment, the boundary between internal and external parties is blurred, making zero trust both easier to implement and more necessary.

Zero-trust, identity-based access is not always possible (e.g., through SaaS solutions that only offer group-based login credentials). Zero Trust is not a Federal Risk and Authorization Management Program (FedRAMP) or ATO requirement - and accreditation is possible without it - but it's a security standard that should be adopted when possible. Similarly to configuration management, zero trust is not something that can be outsourced to a vendor. Since zero trust is a security philosophy, there is no one-step software or tool available for implementing it. Rather, you should first audit your communications chains internally to have the clearest view possible of what a secure connection means in your agency. External vendors can then provide you the tools to make those chains zero trust.

### **Enable Traceability: Logging Your Cloud Utilization**

Keep a record of baseline activity in your organization by capturing and analyzing your agency's cloud usage. This helps identify abnormal patterns that could indicate malicious activity. Always begin with native tools, using a minimal number of third-party providers when possible. Actively monitor and enable all log sources using vendor tools to improve data. A standardized tagging strategy allows you to harness Cloud Security Posture Management tools, which help inform how your agency continually reconfigures its cloud model for purposes like compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization. Finally, enterprise Security Information and Event Management tools can give you live monitoring of security events in your organization.

### **Apply Security at all Layers**

Preference should always be given to FedRAMP provisionally-approved solutions when evaluating cloud-based solutions. FedRAMP approval ensures that a cloud-based solution meets the requirements of maintaining a core set of processes to ensure effective, repeatable cloud security for your agency. Solutions that have already achieved a Provisional Authority To Operate (P-ATO) through the FedRAMP process provide a reduction in effort and time compared to traditional ATO assessment and approval.

Leveraging a FedRAMP option where the Cloud Provider has the greatest security control implementation would provide the least resource allocation. If a SaaS solution is available, or would fulfill the requirements, the majority of the security control implementation has been addressed by the FedRAMP P-ATO. A specific agency's responsibility for security control implementation increases as the cloud model shifts from FedRAMP-approved SaaS, to PaaS, IaaS, to non-FedRAMP-approved products.

If your agency finds it necessary to adopt a cloud service that doesn't meet all of your unique security requirements, you can work with your CSP to develop a Plan of Action and

Milestone Remediation. This process is required for ATO approval, and helps you and your CSP identify potential security risks and outline a plan for mitigation. This process helps your agency make a risk-based assessment of the potential cloud service for your mission needs.

As discussed in the [Governance](#) section, a change management board can help guide the cloud adoption process. For security in particular, either this board or another group within your agency should be used to implement proper governance and compliance, as well as to regularly review firewalls, ports, and protocols. This supports consistent monitoring of potential security risks as well as alignment with your agency's overall change management process.

### **DevSecOps**

You may have unique security considerations if you're migrating development processes to the cloud. Designing your technology stack to take advantage cloud features requires your applications to be cloud native. This compatibility allows you to quickly scale, but the migration process and maintenance of cloud infrastructure requires continual management, or DevSecOps. If your agency already struggles with DevSecOps, introducing an external entity isn't likely to improve your IT management problems. Creating a plan that leverages available security procedures before, during, and after expanding your accreditation boundary is crucial to a secure migration.

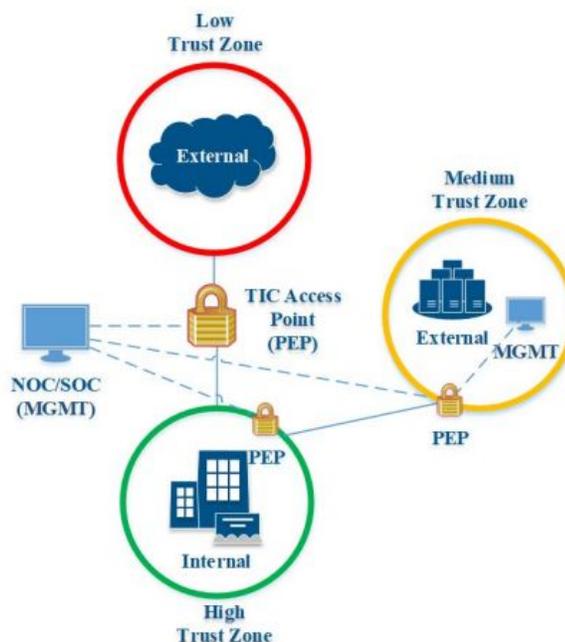
The flexibility of cloud enables rapid repeatable deployments, which DevSecOps can keep secure. Agencies that use Infrastructure as Code (IaC) in particular should look to use DevSecOps best practices as part of their development process. DevSecOps uses version control to make frequent but small changes, and is most relevant for PaaS solutions. A robust and mature configuration management process is needed to integrate this security model into your PaaS development and concepts outlined in the [Governance](#) section will establish a foundation to build on. Someone within your agency should be made responsible for version control to ensure that the most recent, secure version is always available if an application is compromised. These checks and balances will help mitigate security risks in your virtual environment.

Containerization is one tool for performing DevSecOps in a cloud environment, although it should serve as just one example of an adaptation your agency can employ to keep your development process secure during and after your cloud migration. It allows a development team to make frequent code adjustments securely. The advantage of containerization is it enables development to occur on a once or twice a week deployment cycle, only making changes to the code product rather than the establishment of web servers, databases, and operating systems. By 2022, more than three quarters of global organizations will be running containerized applications, compared with less than a third today. Though similar to virtual machines, containers are language- and server- independent (e.g., agile), have shorter lifetimes, and are not directly integrated with physical networks. Your agency

should take into account its unique security considerations when choosing applicable tools like containerization for its migration and cloud management.

### Protect Data in Transit and At Rest

CISA’s Trusted Internet Connection (TIC 2.0) is an existing reference guide that outlines technical architecture requirements for remote access, reporting, and secure data storage and transfer.<sup>45</sup> Reference TIC 2.0 for security best practices and requirements. The latest draft version of CISA’s Trusted Internet Connection (TIC 3.0)<sup>46</sup> provides updated implementation guidance as cloud services become more prevalent in agency information system solution architectures. A major update in TIC 3.0 is the use of “trust zones” (Figure 7), which use multiple compartments to divide your agency’s architecture rather than a single boundary between your data and the internet. These zones are a lightweight implementation of Zero Trust and support more distributed networks across multiple locations and with remote workers.



47

**Figure 7. Trust zones defined in TIC 3.0**

The guidance further incorporates additional policy enforcement points (PEPs), which secure agency-managed trust zones (e.g., cloud service providers). PEPs can be security devices, tools, functions or applications that enforce security capabilities associated with TIC. An individual PEP may enforce all of the security capabilities associated with a given trust zone. Some PEPs may only meet a subset of the applicable security capabilities and

<sup>45</sup> [https://www.doi.gov/sites/doi.gov/files/uploads/tic\\_ref\\_arch\\_v2-0\\_2013.pdf](https://www.doi.gov/sites/doi.gov/files/uploads/tic_ref_arch_v2-0_2013.pdf)

<sup>46</sup> <https://www.cisa.gov/trusted-internet-connections>

<sup>47</sup>

<https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf>

can combine with complimentary PEPs to meet all capabilities. For best practice, prepare to move towards TIC 3.0, if possible.

Traditional network boundaries become much more nebulous in the cloud, which makes protecting network traffic more complex. TIC 3.0 leverages Zero Trust Architecture as a best practice approach to manage enterprise security, allowing users minimal - but sufficient - access to data to contain damage in the event of a security breach. NIST has drafted specific recommendations to implement this architecture, which your agency should prepare to adopt once finalized.<sup>48</sup>

Data at rest can be an overlooked aspect of cloud security. Encrypting data that isn't regularly used by your organization can help keep it secure. All major CSPs offer key management systems for this purpose. In contrast to IAM, which protects against external threats, key management prevents CSPs from directly accessing infrastructure. Encryption keys should be customer controlled to ensure that the CSP itself cannot access data without an audit. Not all CSPs make this seamless, so it may be necessary to use noncompliant tools. Automate regular key rotation and revocation to protect against potential compromises.

### **Prepare for and Prevent Security Events**

When you assess cloud models for your agency, carefully consider the balance between customization and convenience for your cloud. With an on-premise solution, customize every security detail to meet the individual requirements of the information system. However, when the information system moves to the cloud, there's a sliding scale in terms of the shared security responsibility for the agency versus the CSP. As shown in Figure 8 below, the agency responsibility decreases as you move away from on-prem, with the IaaS model retaining the most responsibility, the PaaS model further reducing agency responsibility, and a SaaS model having most security responsibility shifted to the CSP. Shared responsibility models vary between CSPs.

---

<sup>48</sup> <https://www.nccoe.nist.gov/library/implementing-zero-trust-architecture>

Shared Responsibility Model for Security in the Cloud			
On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (platform-as-a-service)	SaaS (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility
  Cloud Provider Responsibility

**Figure 8. Shared Responsibility Model for Security in the Cloud**

Certain security control family implementations will always be the responsibility of the agency. These controls usually include Access Control, which addresses how users are granted access, how accounts are monitored for continued applicability, and how access is revoked when no longer required. Additional examples include how access to data is approved and how least privilege and separation of duty principles are applied.

A responsibility assignment matrix, or RACI (Responsible, Accountable, Consulted, and Informed), helps document and visualize the shared security roles across your agency and your CSP. This will clarify responsibilities and avoid leaving roles and functions unaddressed.

## 6. Target State Environment

One of your most important steps in developing your cloud strategy is creating your Target-State Environment in the cloud. This is a key process and will be your focus once you move beyond the migration and implementation phase of adopting cloud services. The target state environment describes the future, high-level service delivery methodology to support continuous improvement. Capturing the target state objectives clarifies the tools and processes your agency wants to leverage. Stakeholders should define the ideal service delivery state. Your cloud team should ensure the target state meets the service delivery objectives. Align roadmaps to governing IT, agency, federal goals, and mission priorities to further convey value add and measures for progress. They usually include the following activities:

- Define the success criteria and metrics based on the defined business needs.
- Decide on the CSP services that will support service delivery objectives. It's crucial to define the target state by performing an assessment for fit/gap analysis of CSP

services because requirements vary by agency. For example, smaller agencies may have less diversification and may not require multi-cloud strategy compared to larger ones. Some agencies may not have the needs for in-house applications development; therefore, considering CSPs with strong SaaS offerings may be the best choice.

- Identify cloud services that will be used. Once the choices of CSPs are decided, defining the initial set of services that will support the pilot or Initial Offerings Capabilities will give an estimate on cost of services, identify workforce skills needed and other required resources. One strategy is to focus on migrating common services to the cloud. This allows multiple applications and programs to leverage the same service, and reduces duplication of effort for the application teams. Examples include directory services, backup solutions, monitoring, etc.
- Leverage industry DevSecOps metrics and tools to measure continual service delivery improvement.
- Identify further service delivery optimizations beyond the application level, such as breaking applications into reusable microservices to deliver application functionality.

As discussed in the [Governance](#) section, agencies should leverage the Federal Application Rationalization Playbook<sup>49</sup> to develop a structured process of identifying, evaluating and migrating applications and workloads to the cloud. This process answers the key concerns around determining whether specific applications should be migrated to the cloud and should be systematic and align with your organization's business goals and objectives. Once you create a list of cloud destined applications, sequence them and make sure all stakeholders understand the migration process and impacts. It's recommended your Cloud Center of Excellence, or similar group, lead these efforts.

During the planning process, follow the guiding principles below:

- Take a phased approach for cloud migration rather than an "all in" approach. Large-scale, one-time migrations are very complex and are prone to poor cost performance.
- Understand the complexities of the cloud environments you will use. A common pitfall is migrating applications to the cloud without thoroughly understanding the integration and dependency complexities of moving existing applications to the cloud. Complex SAAS implementations require strong risk management foundations, and should incorporate support from expert program management assistance as a best practice.
- Determine the costs associated with a migration. Identify hidden migration-related costs, such as unplanned downtime, contract negotiations, and training.
- Assess each application for cloud fit before migrating. Not all applications should move or can move to the cloud.

---

<sup>49</sup> <https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf>

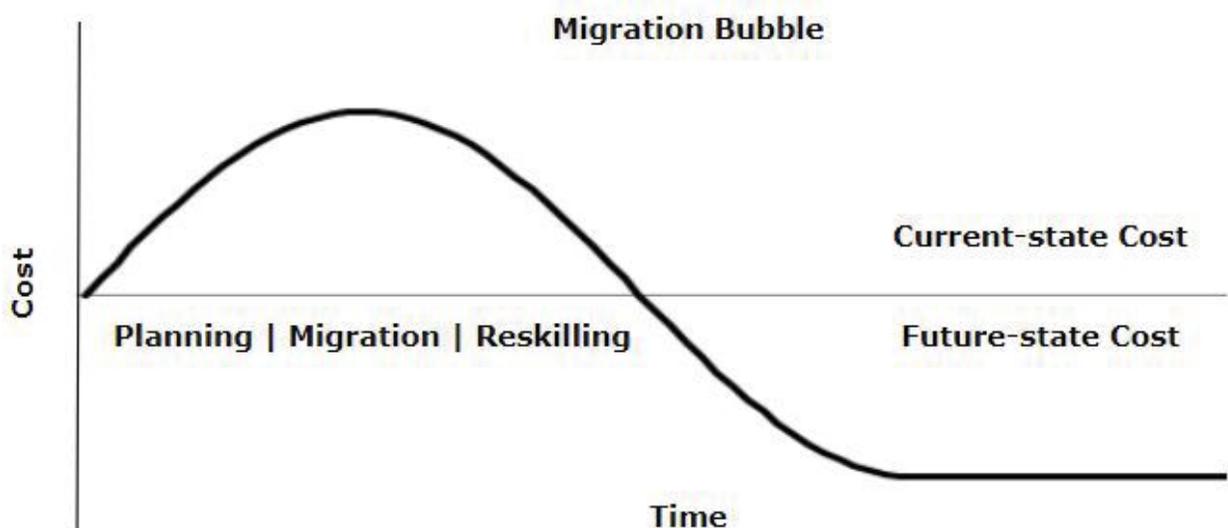
- Create a cost model and plan for variance. Allow for flexibility in the cost model for changes as they happen.
- Involve application and business owners early on. Identify and document the performance, availability and capacity for each application.
- Adopt a business-focused view of your migration objectives.

### Analyze Hosting Alternatives for On-Premise Applications

There are general cost considerations that come with migrating from an on-premise solution to a new hosting environment:

- Assessing the current-state;
- Planning for migration;
- Getting stakeholder buy-in;
- Running parallel systems;
- Vendor management;
- Training and reskilling; and
- Refactoring and replatforming existing applications, if necessary.

Agencies often experience a “migration bubble,” which creates a significant cost increase by running current- and future-state systems in parallel. While the future state shows a rebaselining of costs below the current-state costs, the actual cost of operating future-state systems depends on how many servers and support systems can be decommissioned or consolidated as part of the application rationalization effort. As agencies act on these decisions, they realize the benefits of hosting in a new environment (e.g., increased worker productivity, greater scalability and agility, and operational resilience). This establishes a new cost baseline resulting in eventual O&M and DM&E cost savings, as seen toward the right tail of Figure 9.



## Figure 9. Cost increase and eventual savings from “Migration Bubble”

Hybrid solutions, where applications or systems run in the cloud and on-premise simultaneously, can greatly increase the size of this migration bubble. In such cases, weigh the technological solution against the increase in costs. Given the high cost of running in both environments, a hybrid solution usually isn't the best investment in the long term. However, some vital systems could be worth the increased cost to ensure they are secure before, during, and after migration.

After taking the initial step of “lifting and shifting” a portion of your portfolio to a cloud environment, build out your cloud capabilities over time, but do so with caution. Many applications cannot effectively lift-and-shift into cloud environments without significant refactoring and modernization. Given the limitations of a lift-and-shift approach, we recommend using a containerization or serverless model to realize the full potential of your cloud migration. Lift-and-shift can increase maturity, leading to cost savings, but eventually savings will diminish from increasing your cloud capabilities. Keep in mind that beyond a certain point, marginal improvements in service delivery from advanced cloud services may not realize the cost savings or the benefits described above.

As your automation and abstraction capabilities mature, focus more on mission and service delivery while also streamlining business functions. Automation increases productivity as staff members can spend more time innovating or focusing on other high-priority issues instead of low-level maintenance on applications. As staff productivity increases, there will be less need to hire new, full-time staff. Beyond automation, tools in the cloud abstraction layer have the potential to streamline access to huge amounts of data and improve service delivery, but only certain mission functions will have both the criticality and the data needs to justify an investment in cloud abstraction.

### Develop a Migration Strategy

Below is a high-level overview of how to approach your migration strategy:

- **Restructure the organization** and adjust to required skills if needed. Redefining team members, roles and responsibilities to operate in the cloud environment is essential for a successful transition. Roles and responsibilities may include, but are not limited to, governance, operation management, architecture, networking, security, change management, site reliability, release management, automation, user experience, DevSecOps, procurement, and billing.
- **Re-engineer business processes** to maximize the efficiency of cloud environments. Utilize an established assessment process, such as application rationalization, to prioritize workloads within the roadmap. The processes can be used to ensure cross-pollination and promote collaboration between relevant stakeholders throughout the use of governance boards and charters that explicitly appoint and make room for differing and varying perspectives.

- **Adopt industry best practices** for migration processes. Define the model to transform existing workloads to a target state, such as [Gartner’s “5 R’s”](#) (Rehost, Refactor, Revise, Rebuild and Replace) (Table 2) migration strategy, which requires adherence to industry best practices, such as microservices architecture and containerization. The following table shows the detailed description of each strategy.

**Table 2. Garner’s “5 R’s”**

<b>Migration Strategy</b>	<b>Description</b>	<b>Benefits/Challenges</b>
Rehost	Redeployment of the workload to a similar environment in CSP datacenter. It alters the infrastructure configuration of the workload. Automated or manual tools can be utilized for this purpose.	Faster result of cloud migration solution, but it yields the least benefit because it does not take advantage of cloud computing capabilities.
Refactor	CSP provides the infrastructure, such as containerization, for running the workload.	Reduce learning curve for the development team, such as programming languages and frameworks. This allows you to partially repurpose and optimize workload to support some of the cloud attributes to reduce the cost of rebuild. However, not all cloud attributes will be implemented to take full advantages.
Revise	Modification of existing code to provide support to the requisites of legacy modernization. Then rehosting or refactoring of the options to mobilize to the cloud.	Higher cost and more time consuming compared to the above strategies.
Rebuild	Discard the code and change the existing architecture, which is normally suitable for IaaS, to adopt Microservices architecture and support PaaS.	Assure feasibility to the unique attributes in the CSP. Cost and lock-in are the main disadvantages.

Replace	Utilization of commercial software delivered and disposing of an existing workload.	Investment in the mobilization of a development team is not required. Inconsistency in data syntactic, lock-in and issues in data accessibility are expected.
---------	---	---

- **Setup a change management process** to increase the probability of successful transformation in this long journey.
- **Setup operating processes**, such as workload enrollment/unenrollment, standard operating procedures (SOPs), site reliability, SLAs, user experience assessments, billing monitoring, workforce training, business process reengineering, resource allocation, and capacity provision plans.

### Cloud Networking Strategy

A network connectivity strategy is essential for cloud migration. Conduct a thorough current-state analysis of your networking capacity and employee skill sets as stated in the [Current State](#) section of this document. Successful cloud adoption requires a viable networking architecture and employees with the requisite background to design and manage complex interconnectivity scenarios. From a networking view, the different cloud delivery models are correlated with the level of network exposure provided by the CSP, with SaaS having the least level of exposure and IaaS having the most. The greater level of exposure, the greater the complexity and skill required to manage the cloud environment. Take the level of exposure into consideration when developing a cloud migration plan.

Table 3 below outlines several models/methods of connectivity for different cloud delivery models. It's important to work with your networking teams to determine the best method of connectivity based on the services you will be utilizing and your security requirements.

**Table 3. Cloud delivery model connectivity**

Model for Communication	Scenario	Attributes
Over Internet directly	IaaS, PaaS, SaaS	Cheaper connectivity, lower network availability, no guaranteed connectivity

Over Internet VPN	Data center extension or (Local Area Network (LAN)/ Wide Area Network (WAN) extension) to Virtual Private Cloud instances	Increased security, cheaper connectivity, lower network availability, no guaranteed connectivity
Via Direct Connection through a Colocated Hosting Provider	LAN/WAN extension to the CSP for both Public and Private access	Dedicated connection, guaranteed connectivity with SLAs, cost effective cross connections
Blended into the agency network backbone by a telecommunications provider	Commercial telecommunications direct Interconnect options.	Dedicated connection, guaranteed connectivity with SLAs,

IaaS cloud services require a governance approach as opposed to an ownership mindset that's common at many agencies. Avoid forklifting existing policies and view the new environments as novel. Leverage existing cloud-native capabilities prior to using 3rd party networking technology. Also, rethink how to manage networking costs by focusing on the quantity of data transferred and which networking services are enabled.

Traditionally, networking teams focus on campus, WAN, and data center environments. Your agency's enterprise network engineers should treat cloud network design as foundational and as important as existing networks. As stated previously, your agency requires investments in training for network personnel since IaaS services exhibit many functional, management and operational differences compared to traditional data center networking. Major differences include: provider-specific terminology, lack of Layer 2 connectivity renders devices unable to communicate on the same Virtual Local Area Network (VLAN), and network segmentation is enabled natively.

Consider shifting at least 50% of your employee networking vendor-specific certifications towards CSP network stacks as part of your overall training/upskilling plan. In addition, shift resources towards network automation to improve agility, cross-train network teams with DevOps and cloud teams, and align them with IAC teams. Procuring managed services is also a good option for agencies that face greater challenges when preparing their workforce for cloud adoption.

As your network teams shift from an ownership mentality to governance, set guardrails and create recommended policies relating to networking decisions and avoid controlling all

configuration decisions. One example of a guardrail is to allow the networking team to create guidelines and recommendations for subnet sizes and IP ranges with specific controls to protect production systems and allow non-networking teams to dynamically create logical networks and IP ranges. Another approach is to allow non-networking teams to deploy networking services such as load balancers, while the network teams make specific vendor and software configuration recommendations.

Your network teams should retain several responsibilities even after moving to a governance model, especially the overall responsibility for the network architecture and topology. This includes routing to CSPs and connectivity/peering across multiple CSP. Your networking teams should implement a transit Virtual Private Cloud (VPC)/virtual network architecture to centralize and aggregate connectivity and security controls. This enables your network teams to manage and control the key ingress/egress routing while non-network teams can focus on managing their VPCs.

Additionally, networking teams must reevaluate their approach to costs. The traditional model has consisted of on-time capital investments in networking solutions with no costs incurred until traffic leaves the data center. Today, cloud networking costs are usage-based for the services enabled and data transferred. There's also a variance in network billing for each IaaS vendor and charges can change regionally. To better manage cloud networking costs, your networking teams should collaborate with your storage, backup, and application teams to determine expected usage. Third party CMPs can also help manage and optimize network costs.

In most cases, a small or medium agency would still have networking/voice service needs under contract. CSP connections are another service that could be delivered by a telecommunications contractor under a vehicle, such as Enterprise Infrastructure Solutions (EIS).

## 7. Automation

Automation is a key element that empowers agencies to take full advantage of the benefits that cloud adoption offers. Adding best practices, such as DevSecOps and cloud automation monitoring tools, allows you to fully realize the benefits and enhance your agency's cloud capabilities. Automation can free up agency resources and ensure that cloud services are used more efficiently and effectively. Be sure to describe the operational processes and technology that your agency will implement to operate and maintain workloads in your cloud environment(s) in your cloud strategy. Make sure you align this content with the benefits identified in the [Business Value](#) section of your strategy.

Identify a strategy for automation to prepare for ways to resolve problems or gain efficiencies that could be introduced or available when moving to the cloud, such as the dynamic nature of cost, capability scalability, and operational distribution of workloads

responsibility. Use the sections below to describe how you plan to utilize cloud automation. It's important to have a strong global tagging strategy, which is referenced in the [Governance](#) section. Creating a robust tagging strategy and standards helps with automating services and operational management. The tagging strategy feeds into IAC principles and supports multi-cloud adoption and management. These sections are designed to provide a basic understanding of the major topics related to automation, but you're encouraged to consider other factors when addressing your agency's specific needs.

### **Plan to Implement DevSecOps Practices**

Automation can improve your software development practices, especially if your agency develops and maintains unique applications and tools. Traditional software development life-cycle practices generally include the development teams to perform development, testing, and deployment to production. The environments are designed to create a pipeline that separates the stages for quality assurance purposes. On-premise environments are normally managed manually by an IT infrastructure team to allow development teams to install and configure workloads. Over a period of time, these environments may evolve due to manual software update activities. Issues associated with this evolution can delay or disrupt the workload delivery pipeline. Avoid this by utilizing cloud computing resources to automate the creation of these environments allow the development teams to have the same environments on-demand. This also enables the IT infrastructure team to tear them down when they're not being utilized to maximize cost effectiveness. DevSecOps practices promote a more cohesive collaboration between development, security, and operations teams as they work towards continuous integration and delivery. Planning for DevSecOps adoption should include the following activities:

- **Emulate production environment testing with cloud-computing resources.** An important Quality Assurance (QA) practice is to have multiple environments dedicated to staging the testing process from development until deploying to production. Non-production environments are designed to mimic production environments, but have the ability to scale down when not needed. It's difficult to test production environment issues in a non-production environment because of the data and resources required. This means issues may be ignored or not resolved quickly. Without using cloud resources, you have limited capacity to dynamically scale-up the non-production environment because of the time and resources required for this manual effort. The ability to dynamically scale up and down using cloud computing resources can help solve this problem.
- **Perform Continuous Integration (CI), Continuous Delivery, and Continuous Deployment (CD) with PaaS tools.** Agile methodologies enable IT teams to be more responsive, flexible and produce user-centric products. When teams adopt automation practices for code building, testing, integration, and deployment, you're no longer reliant on manual activities, which increases productivity and quality. Use

PaaS tools available from CSPs to perform CI and CD to save time and resources to perform setup, configuration, and maintenance.

- **Workload monitoring and instrumentation.** Monitor infrastructure environments and workloads to avoid unexpected service interruptions and track this through telemetry services provided by CSPs. Many of these services are used right out of the box and are simple to integrate with workloads and native cloud services. Development teams should include workload-level telemetry as part of the development process so that they have an ability to perform preventive maintenance from the real-time runtime feedback when necessary.
- **Scale non-production environments with cloud resources.** Infrastructure resources capacity planning for on-premise is based on Capital Expenditure (CapEx) practices. A large amount of capital investment is spent and pre-planned to cover the workload demands, some of which may fluctuate seasonally. Plan capacity to cover the peak of demands to avoid any service disruption. As a result of this need, resources are not invested efficiently. Cloud computing resources provide more options to allow Operational Expenditure (OpEx) to dynamically utilize on-demand resources which increase the efficiency. Use cloud resources to scale non-production environments, such as test environments, to perform load testing to match production for a short period of time to get more accurate results.

### **Plan to Adopt IaC Principles**

Cloud computing provides infrastructure management technologies that transform the way your agency can manage IT infrastructure. Adopt IaC to automate the DevSecOps pipeline management empower your agency to achieve the following:

- Changes to infrastructure support are encouraged, rather than being treated as an obstacle.
- Systems are routinely changed without difficulty for users or IT staff.
- IT staff quickly recover from failures without assuming failure can be completely prevented.
- IT staff focus their time on non-routine and non-repetitive tasks that have greater impact.
- Continuous improvements are made instead of expensive and risky big-bang delivery processes.
- Self-service infrastructure for users to define, provision, and manage the resources they need.
- Infrastructure is defined in executable code to implement, test, and measure results compared to just exist in design documents.

There are challenges that come with dynamic infrastructure and automated configuration, which IaC addresses. For example, server sprawl can lead to a number of servers growing faster than the ability for the team to manage. In addition, configuration drift can occur

over time when a number of servers are managed manually, creating variables of configurations that are hard to reproduce and rebuild. Unmanaged variables between servers can lead to snowflake servers, fragile infrastructure, and automation fear.

IaC is not intended as a first step for agencies beginning to approach cloud migration, but is rather a set of best practices for higher-level optimization for agencies that feel they have mastered the basics of cloud. The following IaC principles will help you overcome the challenges cited above. To implement these principles, your CSP needs native tools or CSP agnostic tools, based on open source, such as Terraform, Chef, Puppet, Ansible, etc.

- **Reproducibility:** The ability to effortlessly build and rebuild any part of the infrastructure. This removes much of the risk and fear when making changes.
- **Disposability:** Dynamic infrastructure benefits allow an agency to simply create, destroy, replace, resize, and move system resources on-demand. These capabilities allow systems to make improvements easier.
- **Consistency:** Teams must reproduce identical infrastructure resources that provide similar services consistently. This will help eliminate configuration drift.
- **Repeatability:** Effective IT infrastructure teams have a strong scripting culture and build configuration tasks as scripts so that they can be reproduced and consistently repeated.
- **Continuous Change:** It's impossible to accurately predict how a system will be used in practice and how the requirements will change over time. The dynamic infrastructure in the cloud allows changes to an existing system to be easier and less expensive.

### Managing Multiple Cloud Environments

If you plan to utilize multi-cloud and hybrid cloud deployment models, consider how the operational management complexity would increase and become more sophisticated. Having a robust global tagging policy greatly reduces the burden of managing a sprawling and complex cloud infrastructure. Every CSP has a different taxonomy for service tagging, so it's important to develop a uniform policy that applies towards multiple vendors. Use the suggested taxonomy in the [Governance](#) section to create a common baseline for multi-cloud resource management. A common tagging baseline also helps with adopting a Cloud Management Platform (CMP).

Identify tools that effectively manage the variations of cloud infrastructures within your organization. Use a CMP to manage multiple cloud environments. Whether you decide to use a CMP or not, there are a number of best practices to help you manage a multi-cloud environment:

- **Effectively integrate your internal and external systems** to efficiently manage your multi-cloud services.
- **Enable self-service and the collection of user feedback** to improve and optimize your use of cloud services.

- **Simplify service requests** and better manage resources to ensure you meet compliance with the SLAs.
- **Automate cloud resource consumption reporting** and track spending to help your agency efficiently optimize cloud use.
- **Enhance visibility for cloud resource management** of virtual resources (application, server, storage, and network) and on-demand services.
- **Formalize management governance** of your multiple-cloud environments is in accordance in your agency's internal policies.
- **Allocate the resources and staff needed** to effectively manage security compliance for your hybrid cloud services in a multi-cloud environment.

For additional information on best practices for using a CMP and managing a multi-cloud environment, see the [Automation](#) section in the attached appendix.

## 8. Governance

Establish adequate governance policies and practices to properly manage and maintain your cloud services. Rely on government guidelines and resources, as well as industry best practices to develop your governance strategy. This section provides an overview of industry best practices, which you should adapt to fit your own comprehensive cloud governance framework. These individual frameworks may only address limited issue areas so we recommend agencies review and adopt practices from the listed frameworks in the [Best Practices Appendix](#). The techniques and practices from these leading frameworks provide significant value for service delivery and management at your agency. Having strong processes in place is critical to cloud service adoption, as your agency's operating environment will extend beyond your existing data centers, and can potentially increase the complexity of your IT ecosystem.

Governance practices should also incorporate many of the automation benefits that cloud services provide. Use these automation techniques for monitoring and managing your cloud services to improve efficiency and provide the ability to quickly identify and respond to any service delivery challenges.

A sustainable IT-governance framework must be firmly grounded in change management practices. Change management is foundational in most governance frameworks and is applied to drive execution, validate deliverables, and approve gates. Ultimately, IT governance is about empowering and bringing people together to make value-based decisions for the enterprise.

### General Cloud Governance

You must have a clear plan for the management and governance of security and other operational concerns for the shared responsibility model of using CSPs. The following

steps cover how develop your governance strategy and allow you to factor in agency-specific considerations:

- **Define policies:** Define the goals for your IaaS cloud efforts and develop clear roles and responsibilities for decision making and implementation.
- **Implement preventative controls:** Identify your policies for preventative controls and code policies in your CPS and agency native tools. Automate account creation and define user account creation workflow.
- **Gain total visibility:** Enable and lockdown logging for all cloud resources.
- **Create an audit process:** To implement retrospective controls, establish a continuous and automated audit process. Map policies to tools and automate policy checks and enforcement. Define remediation outcomes and automate remediation workflows.
- **Integrate tools:** Integrate data depositories, implement identity management, and enable SSO.

Aspects of governance also apply to each of the following, major management functional areas:<sup>50</sup>

- **Provisioning and orchestration:** The cloud management tasks used to create, modify and delete resources, and to orchestrate complex deployment and management operations.
- **Service requests:** The tasks required to collect and fulfill requests from business users to access cloud services or deploy cloud resources.
- **Monitoring and analytics:** The collection of performance and availability metrics as well as the intelligence to analyze data that prevents incidents or automates incident resolution.
- **Inventory and classification:** The ability to discover and maintain an inventory of cloud resources as well as the ability to monitor change and manage configurations.
- **Cost management and resource optimization:** The tasks needed to track and optimize spend on an ongoing basis as well as to align resource capacity to actual workload demand.
- **Cloud migration, backup, and disaster recovery (DR):** The ability to replicate data to migrate workload, implement business continuity or DR architectures, or to protect data against accidental deletion or malicious activity.
- **Identity, security, and compliance:** The tasks to manage and secure access to cloud services as well as enforce a security configuration baseline.

It's important to determine your approach early in the planning phases. This allows your agency to identify and source the appropriate skill sets to assist in the governance activities. Many of the governance functions listed are native to a CSPs capabilities, but can also be streamlined via third party CMPs.

---

<sup>50</sup> IaaS Cloud Governance Guidelines and Guardrails for Midsize Enterprises. Gartner. September 5, 2019.

## Engage Agency Cloud Experts

If your agency has the available resources, one best practice is to Establish a Cloud Center of Excellence (CCOE), or similarly organized team of cloud experts, to help your agency successfully execute and manage cloud projects. A CCOE helps your agency develop the right processes and necessary documentation to implement and manage your cloud infrastructure and environments after implementation. It also provides the capability for your agency to scale up your cloud efforts as needed, if you intend to have a phased migration approach of individual applications and databases. Finally, a CCOE can standardize and clarify roles and responsibilities for individuals and teams for the various phases of your cloud projects.<sup>51</sup> While the staff and resources to maintain a CCOE may not be feasible for every agency, smaller agencies can leverage some of the benefits of these centers by following some of the same guiding principles. A formal CCOE is not a requirement, but ensuring that an individual or team, like a Cloud Advisory Services (CAS) group is accountable for the same functions a CCOE would normally cover is a best practice for a successful cloud migration.

Keep the following best practices in mind when you engage and empower your agency's cloud experts:

- **Build expertise and cloud governance capabilities over time.** Ensure your agency documents its best practices from the beginning and take an iterative approach to building the CCOE and policies supporting your cloud activities.
- **Start small and scale up.** Focus on solving internal users common problems across your agency. This will build credibility and lead the cloud team to project success. Gradually expand the scope of the CCOE to take on greater and more complex cloud tasks and initiatives in support of your cloud strategy.
- **Build a team of professions with a breadth of experience.** Ensure you have representation from various functional areas such as security, networking, solutions engineering, etc. Avoid trying to find individuals who can perform all these tasks. This staffing strategy will not yield much success, as these functional areas are broad and very few individuals know them all.
- **Sustain engagement with your users and stakeholders.** Focus on communication and customer engagement to highlight success stories, progress against metrics, and launch recognition programs.
- **Keep expert support high level.** Ensure your team of cloud experts do not support transactional day-to-day cloud operations, such as daily interactions with CSPs. Their activities should align to your strategic business activities.
- **Identify an executive sponsor from leadership.** This will help secure leadership buy-in. The executive sponsor should “market” the CCOE to create widespread recognition of its scope and authority.

---

<sup>51</sup> Ignition Guide to Building a Cloud Center of Excellence. Gartner. June 12, 2019.

The following steps lay out the methods to establish an effective team of your agency's cloud experts:

- **Prepare to Establish the Center:**
  - Lay the foundation for a CCOE by ensuring all stakeholders understand the scope of the process, their responsibilities, timelines, and the expected outcomes.
- **Determine Scope:**
  - Define the CCOE's objectives and develop corresponding success metrics. Sample objectives include: establishing cloud governance policy or providing subject matter expertise for cloud projects. Sample metrics can include number of projects CCOE has assisted or number of policies released in support of the cloud strategy.
  - Define the CCOE's activities around your defined objectives and desired outcomes. Create activities based around the maturity of the CCOE. Create an activity catalogue to outline CCOE activities. Example activities can include actions, such as: architecting cloud solutions, conducting cloud readiness assessments, and assessing and selecting cloud vendors.
- **Build the Team:**
  - Identify a team leader with the requisite cloud skills. Typically, this individual will be a senior staff member who has the ability to lead cultural change, create a cloud strategy and manage cloud implementations. They should have a strong ability to communicate, collaborate and manage vendors if that function is required for the CCOE.
  - Determine team members. Identify roles such as solutions architect, security architect, cloud engineer, finance analyst, network engineer. If resources prevent your organization from assigning individuals full time to this group, you can matrix in other teams and individuals to fill these functions.
  - Define roles and responsibilities of CCOE team members.
- **Prepare to Launch**
  - Develop a communications plan for CCOE engagements with other teams in your agency. Identify stakeholders and develop messages for those stakeholders based on their areas of interest that demonstrates what the CCOE can do for their group. Send your activity catalogue along with your messages.
  - Create mechanisms to sustain user engagement and drive CCOE service utilization based on stakeholder feedback. For example, send newsletters highlighting how employees engaged with the CCOE for project success, display success metrics via a visually appealing dashboard or hosting user networking events.

- Define a cadence to periodically validate or modify CCOE objectives. This will give you an opportunity to redefine the CCOEs role and expand it based on the maturity of your agency cloud adoption strategy.
- **Monitor Effectiveness:**
  - Track effectiveness through surveys, interviews and customer feedback. Modify your CCOE strategy based on these data points.

## Cloud Governance Control Policies

Without written documentation to establish requirements which can be adequately enforced, your agency will fail to have an effective governance strategy for your cloud projects. Without adequate governance for cloud services, you may find it difficult for your agency to effectively determine, report on and reduce exposure to security, compliance and vendor risk. Use the three foundational control policies listed below as minimum requirements for any cloud model.<sup>52</sup>

1. **Approve all cloud use through a defined formal process.** Agency IT and business stakeholders must jointly create a flexible and realistic process for acquiring and using new cloud capabilities.
2. **Require explicit owners of applications to accept risk consequences.** Service owners must formally accept risks associated with the cloud service model. Your agency can accomplish this through the FISMA ATO process.
3. **Maintain a Comprehensive Application Inventory.** Your agency's approval and responsibility acceptance processes must include a formal registration of SaaS, IaaS, and PaaS services and ensure all applications are formally tracked. This can be accomplished in multiple ways (e.g., using a spreadsheet to track existing asset/service management software). At a minimum, you should track the following:
  - Cloud system name and type;
  - Roles such as owner, administrator, support personnel, etc.;
  - FIPS 199 categorization;
  - Contract details;
  - ATO details; and
  - List of services or applications integrated with the cloud service to include applications leveraging APIs.

The majority of IT services are typically acquired through your agency's CIO Office. This process has been the case for the majority of IT solutions in the past, but acquiring SaaS applications can be as simple as using a credit card. The technical barrier to entry for using SaaS applications is so low that individuals in any business unit can easily purchase and utilize them to establish formal processes that govern the acquisition and use of solutions to mitigate unauthorized IT. Your SaaS governance approach should include policy and technical controls.

---

<sup>52</sup> How to Develop a SaaS Governance Framework. Gartner. February 11, 2020.

Reduce the risk of “shadow IT” by using Cloud Application Discovery solutions, which are commercially available either as standalone products or part of a CASB platform offerings. These solutions help identify and manage your agency’s portfolio of SaaS and other cloud applications. When developing your cloud governance model, it’s important to involve your operations and security stakeholders for buy-in and access to existing network and security infrastructure that identifies and places controls on cloud applications, with particular focus on SaaS solutions.

## **Perform Continuous Management**

Ensure your agency is capable to sufficiently maintain these cloud systems and support agency staff using these applications. This includes providing continuous management and support for user activity and having a response contingency plan when an outage or unplanned event takes place. Ensure that agency staff managing cloud systems have an understanding of their clearly defined roles, and feel empowered with the tools and resources needed to perform them. Routine service management consists of the control activities below. Cloud managers should be aware of these activities and trained in accomplishing them.

### **Regular Control Activities:**

- **Vendor risk management:** Ensure service-level agreements (SLAs), performance, quality, and other forms of delivery are being met.
- **Service monitoring and license Management:** Actively manage licenses and license utilization. Vendor charges must be accurate in relation to license usage. Pursue license optimization initiatives (e.g., contract consolidation).
- **Identity and access management (ICAM):** Assist in federating to existing directory services, if possible. Manage accounts on service (e.g., create, delete, suspend, etc.).
- **Compliance reporting:** This activity aligns with FISA ATO requirements based on the system’s FIPS 199 rating. Service management consists of regular data audits and reports to document appropriate safeguards.
- **User activity:** The CSP is typically responsible for monitoring user activity. However, if possible, assign an agency employee to review logs as an additional safeguard. If you intend to leverage automated solutions to enforce SaaS access policies, use application discovery tools to prevent “rogue SaaS access.”
- **Data backup and versioning:** Depending on the system’s FIPS 199 categorization and Incident Response Plan (IRP), your agency must confirm that routine backups take place along with data restoration. If the provider doesn’t provide the appropriate capabilities, supplement the service to meet requirements.
- **Cloud monitoring:** Leverage native cloud solutions to provide monitoring tools, or APIs, and agency solutions to identify issues with mission-critical applications. Monitoring tools help diagnose the scope and source of performance problems and facilitate service resolution with third parties.

- **Annual cloud portfolio review:** Complete this review as part of the portfolio management process. Schedule all cloud applications for an annual review to determine whether they are still necessary, controlled differently, or would benefit from some augmentation or improvement.

### **Unscheduled Management Tasks:**

- **Problem resolution:** Align incident management procedures with your agency's incident management procedures. SaaS customers rarely have direct access to SaaS provider personnel for severe technical issues so be prepared to provide Tier 1 support for minor incidents. Issues that can't be resolved locally will escalate to your agency's CSP. You should have access to self-service portals or resources to resolve simple problems but must be provided access to a support function at the SaaS provider.
- **Service or data recovery:** Have an incident response plan in case the CSP experiences extended downtime, suffers an unrecoverable loss of data, or experiences a business failure.
- **Incident response, investigation and E-discovery:** If possible, request privileged access from the CSP to investigative activities and E-discovery tasks. If access can't be granted, ensure the provider can support your agency requirements through contractual requirements.

### **Manage End of Life (Planned and Unplanned)**

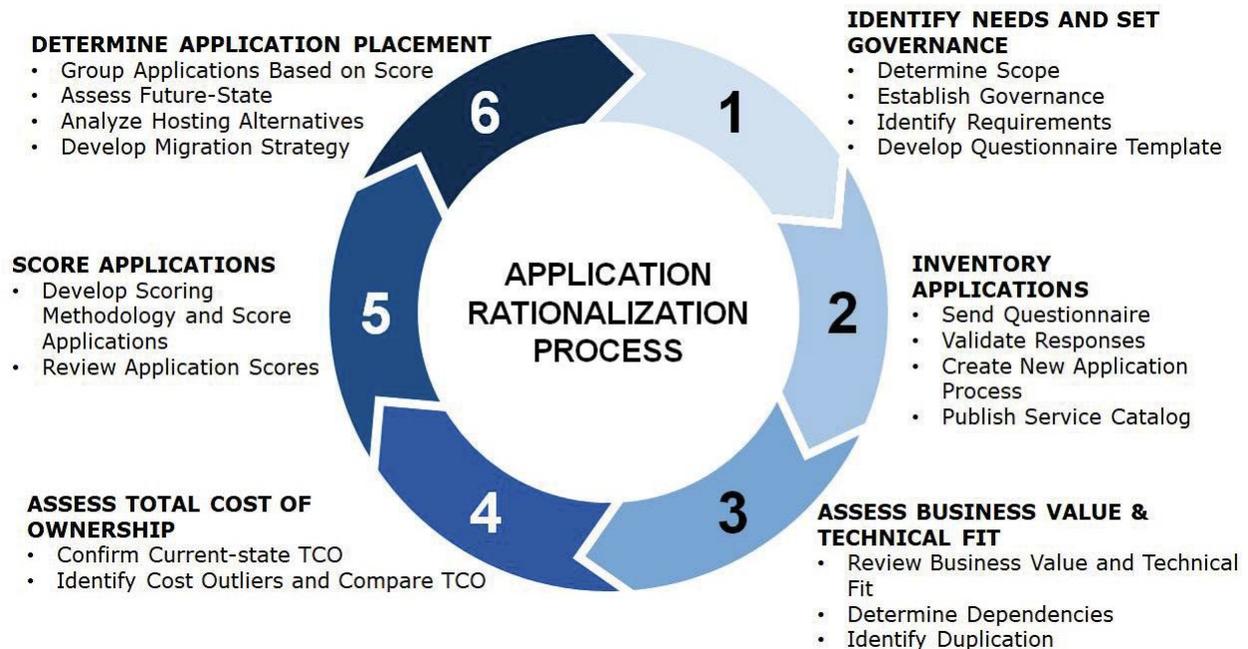
Have a successful approach to manage and maintain your data when removed from your CSP's SaaS environment. Known as an end-of-life plan, this strategy details the final phase of cloud control activities. The plan needs to have steps outlining when and how to shut down a service safely and deprovisioning it before your CSP's contractual obligations end. If a SaaS vendor provides short notice of change or shutdown, or worse, ceases operation without warning, it can leave customers without recourse. While encouraged, an end-of-life plan may not be necessary for all applications that your agency operates and maintains.

### **PaaS Governance**

Developing a PaaS governance strategy consists of a combination of the SaaS and IaaS governance models. A review board for implementing new PaaS modules is the most important governance control for PaaS solutions. The PaaS provider is responsible for the infrastructure stack, from the physical layer to the operating system, while customers are focused on the application layer and up. PaaS solutions tend to be hybrid SaaS/PaaS solutions, which offer SaaS product functionality that can extend through an API and modules, and can be added to the core product. The specific shared-responsibility requirements from your vendor must be thoroughly understood and planned for accordingly. Reference the list of governance tasks outlined in this document as a starting point to manage your PaaS services.

## Application Rationalization

The six-step process below is a structured, iterative approach to application rationalization for IT Portfolio Managers. The six steps provide discrete actions to your approach to the application rationalization process. We encourage you to tailor these steps to meet organizational structures, unique requirements, and mission needs.



**Figure 10. The Application Rationalization process**

**Step 1: Identify needs and set the governance** for the application rationalization effort.

Work with stakeholders such as the agency OCIO, or other enterprise-wide leaders to:

- Develop governance for the effort;
- Establish appropriate decision-making processes;
- Identify the right agency staff to support implementation; and
- Create working groups to provide insight from across the enterprise.

Use existing systems, such as the Capital Planning and Investment Control (CPIC) process, to inform the scope and governance of the application rationalization effort. CPIC provides agencies with a baseline system and corresponding product component inventory that is reported to OMB, sets IT governance structures, and serves as an initial framework for application rationalization.

**Step 2: Inventory the applications** that are in-scope for the effort, and validate against existing application inventory and financial systems of record. This entails sending a questionnaire to stakeholders such as application owners, IT managers, end users, and others across the enterprise (e.g., collectively, “program offices”) who can provide relevant information pertaining to each application and service, including cost data. Having an

authoritative application inventory is critical for IT leaders to make informed decisions and rationalize the agency's application portfolio.

**Step 3: Assess the business value and technical fit** of all applications in the application inventory. Analyze and validate business value and technical fit information captured in the questionnaire sent to program offices in Step 2. Engage program offices in an iterative manner to ensure collaboration across the enterprise. Review the application inventory for dependencies and duplication to enable informed rationalization decisions.

**Step 4: Assess the total cost of ownership (TCO)** in collaboration with the program offices for all applications in the application inventory. TCO information is captured in the questionnaire sent to program offices in Step 2. Compare TCO in the current-state against estimated TCO in future-state architectures.

**Step 5: Score applications** based on the business value, technical fit, and TCO information gathered in Steps 3 and 4. This provides relative scores for all in-scope applications, and helps determine whether an application should be reviewed, rewarded, removed, or refreshed (note these are non-technical terms).

**Step 6: Determine application placement** based on the application scores and other pertinent information gathered throughout this process, including input from stakeholders. Program offices then develop and execute an iterative change management and application migration strategy.

## Naming Conventions

Cloud automation allows for rapid scaling and flexibility. Managing thousands of servers or devices can be a challenge if your agency does not have a standard taxonomy to identify these services. If your agency does not have a standard for naming conventions, it is highly recommended you create a standard prior to IaaS adoption. There are many approaches to defining a standard for your agency; work with your governance teams and operations teams to define the taxonomy. The following taxonomy can be a starting point for your agency: Country Code, Location Code, Unique Site Code, Device Role, Service Level, etc.

## Cloud Tagging Strategy

For large-scale cloud environments, especially those on IaaS platforms, tagging is an essential element for a cloud automation and government strategy.<sup>53</sup> Adopt a standard tagging framework based on several categories, including the four below:

---

53

<https://www.greenhousedata.com/blog/implement-cloud-tagging-to-simplify-automation-and-administratio>  
[n](#)

1. **Technical:** Includes information such as, the application running on the resource, what cluster it belongs to, or what cloud environment it runs in (e.g., development, staging, etc.).
2. **Automation:** Tags that can be read by automation tools, including planned decommission dates, what versions of scripts or software packages to install, etc.
3. **Business and billing:** Tags to track which business unit or individual owns a resource, which units or customers the cloud resource is providing services for, or an assessment management ID.
4. **Security:** Tags to assist with compliance, information security, and access controls.

Once you develop and implement a standardized tagging strategy, you can use them for both native and third-party automation tools for several purposes:

- **Configuration management:** Use tags to change settings and install software packages.
- **Chargeback and accounting:** Correspond specific cloud services to specific lines of business .
- **Continuous improvement:** Tag build numbers and code repositories to bolster your CI/CD efforts.
- **Improve organization:** Identify and retire resources that are redundant or no longer used.
- **Enhance compliance and security:** Manage and ensure compliance for cloud resources and protect sensitive data.

Use a common-denominator approach to your tagging strategy for multi-cloud environments. Additional guidance is provided in the *Appendix: Best Practices* for specific details and examples of foundational tags your agency could use.

## 9. Finance

Focus your organization on cloud financial management and optimization. Many agencies move to cloud services assuming cost savings will automatically materialize. In some cases costs are cheaper but, more often than not, they're similar to on-premises computing models (if not more). Even if costs are similar or higher, there are many advantages to cloud services, as outlined in the [Business Value](#) section of this document. It's important to devote time and resources towards conducting a thorough business case and total cost of ownership for workloads and applications destined for the cloud.

Cloud billing can be complex, especially IaaS services. There are numerous configuration and service options for users. If services are incorrectly configured or there's a lack of management oversight, your agency can be faced with significant cost overruns. CCOE

team members with familiarity with cloud billing will pay dividends in the future as your agency adopts more cloud services.

Cost drivers for cloud vary by service model. You need a thorough understanding of your DR and COOP criteria, application workload, and response-time demands to choose the correct model for your agency and meet your mission needs. Table 4 identifies some common cost considerations associated with each cloud delivery model. It's important to note that many companies offer more than one mode even though they are considered only in one space.

**Table 4. Common cost considerations by cloud delivery model.**

SaaS	PaaS	IaaS
<p>If billed per user, variable cost can sway considerably, depending on the size of your agency.</p> <p>It's worth evaluating whether the price of unlimited service beats the variable cost of being billed per user if you have an "all you can eat" contract rather than per user.</p>	<p>Billed in number of calls or milliseconds.</p> <p>There are add ons from the provider or a third party. These are akin to smartphone apps and some come pre-installed, while some are billed through your provider.</p>	<p><i>Compute:</i> The equivalent of servers and usually billed in minutes or hours.</p> <p><i>Storage:</i> The equivalent of disk space, which varies depending where it is on the spectrum of long-term versus ephemeral storage.</p> <p><i>In-and-out bandwidth:</i> Data out charges vary depending where it is on the spectrum of long-term versus ephemeral storage.</p> <p><i>Third-party tools:</i> These are purpose-driven, pre-configured servers, which are used per minute/hour using the IaaS building blocks (e.g., a computer server with facial recognition software installed).</p> <p><b>Additional but less central IaaS drivers include:</b></p>

		<p><i>Transactions:</i> transactional charges within the solution's ecosystem.</p> <p><i>Connectivity:</i> charges related to ecosystem connectivity (e.g., having a static IP address for a server).</p>
--	--	---

### Monitoring Spending with Tagging

It's important to carefully choose a cloud service model as your first step towards financial management, but the agility of cloud service means its financial costs and benefits are constantly changing. A standard tagging taxonomy helps monitor cloud spending, both for reporting purposes, as discussed in the [Governance](#) section, but also for successful financial management. Use the Technology Business Management (TBM) framework<sup>54</sup> as a standardized way of managing cost, quality, and value of IT services.<sup>55</sup> Its wide adoption makes it a logical choice for uniformity across agencies, and it provides transparency into the infrastructure and applications that data centers support. Tagging for cost optimization and tracking allows you to monitor expenses in otherwise nebulous service models. As described in the [Governance](#) section, a standard tagging framework and taxonomy is crucial to cost optimization and helps you better understand how, and for what purposes, the cloud is being used.<sup>56</sup>

Use tagging to continually reassess your agency needs and avoid wasteful spending on cloud resources. Cost optimization requires constant IT Demand Management, which many agencies fail to fully grasp, even in non-cloud aspects of their IT portfolios. IT assets which initially fit cost and effectiveness criteria may create unnecessary costs if they're not properly repurposed for new requirements, or, even worse, can mean extra management and maintenance fees if they're not properly terminated when no longer needed.

Application workloads regularly change and the most efficient cost model now may not remain the best choice as needs shift to meet mission demands. For instance, if you chose a model based on a workload that's steady around the clock but then noticed a pattern of peak hours, a switch to an on-demand service may be more beneficial. Likewise, if you anticipate widespread use of a software, but employees only use a handful of tools, a more lightweight Feature-as-a-Service (FaaS) solution may be more cost effective.

<sup>54</sup> <https://www.cio.gov/2020-09-30-New-Maturity-Model-Increases-IT-Spending-Transparency/>

<sup>55</sup>

<https://www.nist.gov/system/files/documents/2017/05/12/doc2017financialmanagementconference-tbm.pdf>

<sup>56</sup> <https://cloudserviceevaluation.com/2017/04/13/the-third-law-of-cloud-cost-optimization/>

Monitoring includes keeping an eye out for “zombie resources,” resources your agency no longer uses. Unused IP addresses, databases, and unused accounts can represent both zombie costs and security risks if you’re not tagging and monitoring resources. For user accounts, an “Owner” tag is an important feature to detect resources employees abandon when they change or leave positions. Similarly, tagging to manage storage and information lifecycles is even more important with cloud usage because it’s easier than ever to use more storage than necessary. Since you’re charged monthly for what you store, failing to archive unnecessary files and data means compounded costs. Storage management doesn’t have to mean file deletion, however; costs can be reduced considerably by migrating lower-use assets to “infrequent usage” tiers or long-term storage options to help you save while preserving your files.

Cloud usage, with many service models, refers to resources a customer allocates to themselves, not necessarily their day-to-day usage of those resources. This presents a unique financial challenge because cloud service providers have little incentive to inform you of the unused resources they bill you for. The responsibility of monitoring those resources falls on you, the consumer.

### **Automate Using Native Tools**

A good approach to effectively monitor usage is to use native CSP tools to automate cloud usage whenever possible. Dynamic automation tools can manage, reallocate, and optimize cloud purchase options based on how your agency is using its cloud resources. Automated solutions have the capability to be far more dynamic than manual methods and can automatically scale to match capacity needs. Many solutions are also able to automate security and compliance risk features and can scan for best practices or alert you of abnormalities that may be signs of a larger problem.<sup>57</sup> If your CSP does not provide these tools natively, many comparable third-party tools are available. It’s also highly recommended to use third-party tools to manage multiple CSP environments. This allows for a holistic financial view of your enterprise cloud portfolio and may provide greater capabilities over native tools.

As helpful as automated tools can be, they do not fully replace manual monitoring. This may mean eliminating the need for Excel for back-end data storage and processing, but does not allow for hands-off management of cloud utilization. An effective cloud billing model is one that utilizes automation as much as possible for small changes, while providing user-friendly insights into your cloud usage for your financial analyst or cloud-portfolio manager.

### **Leveraging a Cloud Financial Administrator**

---

57

<https://www.gartner.com/en/documents/3982411/how-to-manage-and-optimize-costs-of-public-cloud-iaas-an>

A best practice in cloud financing is to designate a financial analyst to strategically manage the use of cloud.<sup>58</sup> This position should take charge of a number of measures aimed at best preparing for financial success. To start, strategically choose a service model based on your agency-usage parameters and complete an initial assessment of your data needs and assets. Include in this assessment an inventory of license agreements. License migration and abandonment each have different financial implications, as well as an ICAM gap assessment to best plan for access management needs.<sup>59</sup> Similarly, be sure to retain account ownership prior to moving resellers. Lifecycle management is crucial to avoid being caught without a service provider at the end of a cycle, which can be an expensive and damaging mistake. Another step that can be taken prior to an agency's migration is an internal infrastructure assessment. Align cloud adoption with the depreciation life cycle of existing infrastructure to smooth the transition financially, especially when coordinated with planned replacements of in-house hardware.

Since the use of cloud services varies with agency behavior, it helps to incentivize financial responsibility within an organization by gamifying or otherwise publicly noting successful conservation efforts. While this should not be a primary cost management method, it can help to increase internal awareness of the relationship between usage and the agency's financial success.<sup>60</sup>

### **Indirect Financial Considerations**

A number of costs, which may not be reflected in the upfront cost of service, indirectly affect the financial management of cloud migration. Many of these costs can significantly impact your budget. A big consideration is your workforce's ability to adapt to cloud usage. It may be necessary to train or augment existing technical expertise, either through hiring practices or internal employee training. Alternatively, strategically choose a cloud service based on their existing human capital and its technical expertise. Another way in which cloud can unexpectedly affect costs is through its impact on network bandwidth. Increased usage to support cloud service can be significant.

Cloud computing does not entirely eliminate the need for data centers and other technical infrastructure, a financial consideration that may not be obvious. In the public sector, it's unlikely that any agency can entirely migrate to the cloud. Disaster recovery and continuity of operating plans provides a need for backup data centers in case of emergency, especially since many agencies are distributed across a number of different cloud

---

58

<https://www.channele2e.com/business/enterprise/cloud-financial-administrator-a-must-have-for-enterprise-cloud-users/>

59

[https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM\\_Roadmap\\_and\\_Implem\\_Guid.pdf](https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf)

60

<https://www.gartner.com/en/documents/3982411/how-to-manage-and-optimize-costs-of-public-cloud-iaas-an>

platforms, complicating DR and COOP. Internal infrastructure management is similarly necessary for contractual purposes. A strategically positioned and risk tolerant enterprise portfolio is needed to manage unexpected contract expirations or cloud companies going under unexpectedly. These in-house data centers also insulate against service-cost changes or additional premiums, which are possible given the early-stage, cloud-service market.

Cloud computing can incur significant savings in the long run, offering greater budgeting agility and reduced fixed costs for infrastructure. Agility can, however, mean unexpected variable costs, which can catch your agency by surprise without careful monitoring. Cloud savings are also not immediate, and the savings horizon can be longer than expected depending on your service model's subscription fees. This horizon can also lengthen by the transitional costs needed to switch to new services, especially services like SaaS solutions, which can require workforce wide training.

## 10. Exit Strategy

Developing an exit strategy for your cloud services is a crucial part of your agency's cloud strategy, and can help avoid the challenges associated with vendor lock-in.<sup>61</sup> The cloud exit strategy ensures you're able to maintain business continuity and take advantage of changing market opportunities without becoming overly reliant on a single CSP vendor. An exit strategy can also protect against unforeseen challenges with your CSP, such as struggling to provide a reliable, secure cloud experience and respond better to organizational business drivers. Conduct exit strategy planning as an initial action rather than waiting until a challenge or problem occurs. This prepares you to take these additional considerations into account when developing a migration and implementation strategy. Having a ready-to-go cloud exit strategy not only increases your cloud and CSP choices, but ensures continuity of mission systems and applications in the cloud by reducing the negative risks resulting from vendor lock-in.

Include a comprehensive analysis of your contractual, technical, legal, and data governance considerations of your cloud systems in your agency's exit strategy. This includes factors such as the cost of scaling up or down, infrastructure management, and data management responsibilities. Workforce factors can also add to hidden costs. Consider the following factors in your exit strategy:

- Organizational readiness;
- The procurement process for new cloud services; and
- Preparing employees for alternative CSP environments.

---

<sup>61</sup> Lawton, George, "Beat vendor lock-in with a cloud exit strategy," January 20, 2020. <https://searchcloudcomputing.techtarget.com/tip/Beat-vendor-lock-in-with-a-cloud-exit-strategy>

Your agency's cloud model determines the outcome of your exit strategy. Migrating and relocating an IaaS application and data is more straightforward compared to PaaS or SaaS solutions. With PaaS, your cloud-native apps need to be refactored to move off the CSP and may require increased development work. Your exit strategy for a SaaS solution may be even more complicated because SaaS providers are more involved with managing and processing data, than IaaS and PaaS providers; specifically with how the data is structured and where it resides. Migrating data when changing CSPs is complex so it's important to review your agency's contractual data ownership and management language.

There are a few additional factors to consider for moving an application back from the cloud to your agency's on-prem resource. You should already have an archived copy of the application that was saved prior to the initial cloud migration. If the application has been refactored, you will need access to this archived copy. In addition, data mapping between a cloud application and a legacy non-cloud application should be continuously updated to ensure a seamless exit from the cloud. Develop data translation tables for the non-cloud application to prepare for exit from the cloud.

You'd normally involve external entities, such as CSPs and Resellers, to provide managed services. The transition from both entities require up-front planning to avoid situations that are hard and costly to exit. A hybrid/multi-cloud model may be required for this strategy with technologies and architectures which are cloud agnostic. It's important to understand the associated risks and costs before making decisions because not all elements in the cloud implementations can easily transition to another CSP. Maintaining consistency and objectives is required for regular and iterative updates to avoid implementation that derails from the plan. The cloud exit strategy guidance framework from [Gartner](#) includes the following best practices, coupled with phases and activities, listed in the table below, with guidance for a federal agency context.

Utilize your agency's existing cloud management team, or designated group, to develop a framework that decides whether to exit a specific CSP or Reseller after specific events or outages transpire. This framework establishes the cloud team that's responsible for responding to the unexpected events and provides exit planning assistance to stakeholders. It's the cloud management team's responsibility to create an agency-centralized repository to maintain exit plan documents for all CSPs and Resellers. Share these documents across programs and offices to inform others and learn from the experience.

Assess your existing workloads based on the cloud deployment models. Each model has a different exit viability, with IaaS having the highest flexibility and control for an agency compared to PaaS and SaaS. However, the infrastructure transition is faster if a CSP provides the same services in PaaS or SaaS. The exit viability is low and very costly to move if your focus is to exit a SaaS product. Perform a thorough risks analysis before making decisions for the products. Include the viability for application migration mentioned in the

[Target State](#) section. Finally, review and assess the data to be migrated.

### Phase 1: Define High-Level Exit Strategy

Activities	Guidance for a federal agency
Assess Application Dependencies	Complete the Application Rationalization assessment ( <a href="#">Target State</a> section) to ensure workload dependencies are recorded in your repository. This information is used in the next activity. Categorize dependencies as “technical fit”, “business values”, “acquisition/procurement”, and “compliance.”
Identify Co-dependent Applications	Part of the assessment from the previous activity, identify the co-dependent workloads to identify constraints or impacts, such as data transfer costs, workload performance, networking costs, that may happen after the transition.
Define Unacceptable Application-Level Events	Define measures of unacceptable events at the workload level, such as significant outage, performance degradation, lower published SLAs, and data loss.
Determine Appropriate Action for Each Event	Identify the appropriate counter-measure actions for the previous activity to determine the proposed alternative hosting options. Actions include: <ul style="list-style-type: none"> <li>● Stay with the current CSP and Reseller expecting an improvement in services</li> <li>● Add additional CSP and Reseller to incorporate as part of the multi-cloud model</li> <li>● Replace existing CSPs and Reseller with new ones</li> <li>● Move the workloads back to an agency private cloud as part of the hybrid cloud model</li> </ul>
Determine if Event Requires Exit From the Provider	In a repository, keep track of each event from previous activity and its impact and evaluate the potential impacts on proposed, alternative hosting decisions.
Evaluate and Select Alternative Providers	If the evaluation indicates an exit is required, perform the alternative analysis evaluation on the new CSP or Reseller using the Application Rationalization and cloud migration frameworks described in the <a href="#">Target State</a> section.
Prepare for Business Continuity	If immediate exit is required, define how to continue to provide services to its users. Exiting an existing CSP or Reseller can have a major impact on business continuity.

## Phase 2: Build Application-Specific Exit Plans

Activities	Guidance for a federal agency
Exit Plan Components	The workloads identified in your exit plan repository should contain a workload movement plan to take you from your existing deployment model (IaaS, PaaS, SaaS) to the target CSP deployment model. This includes the application, data, and security requirements. Your workforce skills plan, a required element of the Cloud Strategy Template, is crucial to a smooth exit from one CSP to another. If you have development teams, the contract clause and language for data and application ownership needs to be clearly stated in your favor to reduce the Resellers resistance to cooperate with the transition.
Estimate Time and Costs	The exit plan should include cloud services costs, software licensing, intercloud/hybrid data transfers, workforce costs, DME, O&M, infrastructure, and contract preparation costs. Include time estimates to account for possible communications and process delays between offices within the agency such as OCIO validation of software licensing, new CSP connection for Cloud Access Point (CAP), ATP/ATO, workforce training and new contract RFI/RFP processes.
Create Backup/Restore Plan	Have a comprehensive Backup Restore Plan for identified workloads from the agency's exit plan repository can facilitate workload movement from one CSP to another.

## Phase 3: Implement the Exit Plan

Activities	Guidance for a federal agency
Update Business Continuity and Disaster Recovery Plans	Moving to a new CSP or Reseller requires an updated business continuity and disaster recovery plan for that workload.
Eradicate Cloud Remnants	Decommission the workload from the previous CSP or Reseller after the successful exit. The cleanup process includes removing cloud infrastructure, platforms, native services, software, data, backups, and snapshots. All security-related data, such as:

	<ul style="list-style-type: none"><li>● Shared, public, and private encryption keys;</li><li>● identity accounts;</li><li>● all telemetry and monitoring data, such as log files;</li><li>● Any cloud brokerage services; and</li><li>● Any other chargeable items.</li></ul>
Severe Provider Relationships	Once the decommission process is complete, review contract termination clauses for the CSP and Reseller to eliminate possible legal issues.

# Appendix I: References

## Cloud Computing Definition

The following Cloud Computing definition is referenced from NIST Special Publication 800-145 “The NIST Definition of Cloud Computing.”<sup>62</sup>

### Essential Characteristics:

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling. The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability<sup>1</sup> at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

### Service Models:

- Software as a Service (SaaS). The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure<sup>2</sup>. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

---

<sup>62</sup> <https://csrc.nist.gov/publications/detail/sp/800-145/final>

- Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.<sup>3</sup> The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

#### **Deployment Models:**

- Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

## Appendix II: Best Practices

The following links are additional resources for cloud best practices:

Cloud Cost Considerations:

<https://cioknowledge.max.gov/?q=system/files/attachment/Key%20Cloud%20Cost%20Considerations%20v1.2%20508.pdf>

Cloud Readiness:

<https://cioknowledge.max.gov/?q=system/files/attachment/Cloud%20Readiness.PDF>

Data Center Migration, Consolidation, and Closure Guide:

<https://cioknowledge.max.gov/?q=system/files/attachment/DCOI%20Guide%20for%20Data%20Center%20Migration%20Consolidation%20and%20Closure.pdf>

Open source risk framework:

[https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=919234](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919234)

Risk Resources Good project management increases the predictability of the outcome and reduces the variation within Result, Scope, and Performance.<sup>63</sup> In order to increase the predictability of project delivery, ask these eight questions:

1. What can vary positively or negatively more than 5% from what is expected?
2. What surprises have we encountered in the past on this type of project?
3. What can go wrong?
4. What else can this cause to go wrong?
5. What can go extremely well?
6. What else can then go extremely well?
7. What do we not know?
8. What do we not know we do not know?

These eight questions flush out potential variation, Risk. These questions generate possibilities that allow us to ask further: Is there variation? Is it positive or negative? What would cause that variation? We then can pursue that variation to its source or its cause.

---

<sup>63</sup> <https://www.pmi.org/learning/library/capturing-project-risk-produce-results-control-8266>

## Procurement Resources

For best practices around creating effective contracts, see the joint document published by the CAO and CIO Councils<sup>64</sup>. For additional procurement resources, please see the [Cloud Information Center \(CIC\) website](#) or contact GSA through the CIC.

## Workforce Resources

### Cloud Dream Team Member List

The purpose of this document is to provide agencies with guidance on assembling pre-migration, migration, and O&M teams for all phases of a cloud adoption based on recommended roles. This team member list outlines the skills and expertise an individual should possess to effectively perform key tasks for respective roles as part of a cloud dream team. The team members which comprise the list were identified based on research, current trends, and industry standards.

### Technical Dream Team Members

Technical team members are instrumental in executing cloud adoption. Although it is recommended that agencies build a full dream team with all positions listed in this document, the team of technical members (4 positions) possess the skills and knowledge needed to undertake cloud adoption for all phases.

Cloud Adoption Manager	
Role	Individual who acts as the POC for the cloud strategy and adoption effort from migration up to O&M, and manages financial, business, and technical processes. Responsibilities include leading the development of cost models, business cases, IT strategies, and value metrics for cloud adoption; applies Agile methodology to incorporate stakeholder input through an iterative process aligned to key milestones.
Required Skills	Experience with cost modeling and tracking, defining SLAs, workload placement, defining continuous improvement reporting and Agile methodologies. Project management skills including team communications, planning and risk mitigation.
Reskilling	Titles: CTO or deputies
	Existing Skills:

<sup>64</sup> <https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/cloudbestpractices.pdf>

	Potential Training: <a href="#">Cloud Costs Considerations white paper</a> , <a href="#">IaaS Considerations for the Data Center Community white paper</a> ; Agile methodology
Phase(s)	Pre-Cloud Migration; Cloud Migration
Position Description Keyphrases	Developing a cloud strategy; business case for the cloud; cloud vendor selection and management; background in Agile

Cloud Solutions Architect	
Role	Individual(s) who have broad knowledge of available cloud services, and how they interoperate; responsible for overseeing an agency's cloud computing strategy including cloud adoption plans and cloud application design, and cloud management and monitoring.
Required Skills	Knowledge of operating systems, networks at the enterprise level, cloud security, and background in programming languages.
Reskilling	Titles: Enterprise architects
	Existing Skills: Experience working with CSP vendors, engineers, and developers
	Potential Training: N/A
Phase(s)	Pre-Cloud Migration; Migration; O&M
Position Description Keyphrases	Participation in all aspects of the software development life cycle; design, build, and deploy cloud applications.

Cloud Network Analyst	
Role	Individual(s) who oversee and lead efforts to identify, manage, and protect the agency's network connections before and after the agency moves to the cloud.
Required Skills	Knowledge of architect virtual networks, access, and resiliency in a cloud environment.
Reskilling	Titles: Network Administrators, System Administrators
	Existing Skills: Knowledge of and experience working on the agency's existing network topology.

	Potential Training: Cloud Networking Certification
Phase(s)	Pre-Cloud Migration; Cloud Migration
Position Description Keyphrases	Network design and mapping; experience integrating systems across agencies and/or bureaus, and troubleshooting system and networking problems

Security Lead	
Role	Individual(s) who are responsible for effective operational security risk management across the agency by identifying security risks, planning and implementing risk mitigation efforts, and preparing for future risks within the cloud space.
Required Skills	Background in federal government IT security including, but not limited to, experience with Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology cybersecurity frameworks, and guidance. Experience in web proxy or firewall implementations. Skills in federating identities (e.g. SAML or OAUTH).
Reskilling	Titles: IT security leads; CISOs; incident review personnel
	Existing Skills: Prior knowledge of and experience deploying cloud security solutions
	Potential Training: FISMA compliance training, Trusted Internet Connections training, <a href="#">Cloud Security Alliance</a> certifications
Phase(s)	Pre-Cloud Migration; Cloud Migration, O&M
Position Description Keyphrases	Application-level vulnerability; experience with mitigating security breaches; identify new attack vectors

**Process Dream Team Members**

Process team members possess expertise to support the technical team’s efforts. These roles typically require a specific set of skills or experience that focus on managing and addressing challenges associated with people and processes.

**Change Management Specialist**

Role	Individual(s) who are tasked with guiding the culture and process changes needed for successful cloud adoption agency-wide. Facilitate collaborative working relationships among stakeholders to ensure changes are implemented as a unified effort; prepare users to adopt the new system and tools; identify risks associated with cloud adoption, and identify and help execute mitigation steps.
Required Skills	Experience working with key stakeholders to help promote a clear understanding of the changes that will take place and their roles in implementing these changes. Background in communications, training, facilitation, business process redesign and user adoption. Prior experience performing change management for an organization adopting cloud technologies.
Reskilling	Titles: Change management specialist; SES ECQ 1
	Existing Skills: Knowledge of existing organization
	Potential Training: Certified Change Management Professional (CCMP); <a href="#">ECQ 1 competency</a>
Phase(s)	Pre-Cloud Migration; Cloud Migration; O&M
Position Description Keyphrases	Leading collaborative, dynamic planning processes; provide recommendations based on comprehensive research; experience instilling organization-wide changes; develops new insights into situations; questions conventional approaches; encourages new ideas and innovations

<b>Cloud Governance Lead</b>	
Role	Individual(s) who provide strategic oversight, develop and enforce the governance rules for team members responsible for systems, applications, and data in the cloud space. Streamline processes and maintains quality control for the agency's cloud effort by ensuring accountability and compliance to procedures during all phases of cloud adoption.
Required Skills	Background in enterprise governance and documentation, drafting and implementing standard operating procedures, performance management, quality management; Knowledge of quality control best practices for cloud adoption.
Reskilling	Titles: Enterprise governance leads; enterprise architects

	Existing Skills: Knowledge of existing IT governance
	Potential Training: N/A
Phase(s)	Pre-Cloud Migration; Cloud Migration
Position Description Keyphrases	Formulating proper documentation; instilling a culture of accountability; enforcing policy

**Site Reliability Engineer (SRE)**

Role	Individual(s) who are responsible for developing scalable and reliable systems relevant to the cloud operations. SREs develop software systems to address operations problems, specifically developing automated and reliable solutions through software engineering.
Required Skills	Experience managing system availability, latency, performance, efficiency, monitoring, emergency response, and capacity planning;
Reskilling	Titles: Enterprise architects; system administrators; system engineers; software developers
	Existing Skills: Configuration management, test integration, and customer support
	Potential Training: Agile methodology; Systems Development Life Cycle (SDLC) training
Phase(s)	Pre-Cloud Migration; Cloud Migration; O&M
Position Description Keyphrases	Modern programming languages; ensuring strategic alignment of technical design and architecture to meet business growth and direction; automation of day to day ops processes

**Release Manager**

Role	Individual(s) who are responsible for managing, planning, scheduling, and controlling the process by which cloud related software is moved from the requirements phase, through the development and testing phase, to eventual deployment and delivery for users.
------	---

Required Skills	Experience with multi tier release cycles, build/release tools (like Jenkins) and source control systems (like GitHub/Gerrit); experience with process tools (like Jira)
Reskilling	Titles: Software developer; release manager; enterprise architect; release engineers
	Existing Skills: experience with waterfall and agile methodology
	Potential Training: waterfall and agile training
Phase(s)	Pre-Cloud Migration; Cloud Migration; O&M
Position Description Keyphrases	Manages releases; deploying code releases; release readiness reviews; coordinates testing

Automation Engineer	
Role	Individual(s) who are responsible for designings, programming, and testing automated machinery and processes.
Required Skills	Hands on experiences using tools to support IaC, working knowledge of design patterns such as Immutable Infrastructure.
Reskilling	Titles: Automation engineer
	Existing Skills: Experience with CSPs; familiarity with configuration management tools (e.g., Ansible, SCOM)
	Potential Training: N/A
Phase(s)	Pre-Cloud Migration; Cloud Migration
Position Description Keyphrases	Experience with virtualization technology; written and maintained automation content; set up process standards for software

## Optional Team Members

These optional team member roles are incorporated into the team based on the following factors: A DevOps Advisor is added to the team if an agency lacks an iterative DevOps process, a Facility Lead would be added to the team if the agency anticipates that the usage of on-premise data centers will need to be modified based on data and applications

being transitioned to the cloud, and a Procurement Lead would be responsible for handling procurement issues that arise from cloud adoption.

<b>DevOps Advisor (if applicable)</b>	
Role	Individual(s) who are tasked with establishing and maintaining the DevOps processes for the software development team throughout the cloud adoption process. Provides technical leadership in creating new and improving existing workflows within agile software development lifecycle, leverage stakeholder requirements in the creation of quality control processes.
Required Skills	
Reskilling	Titles: Cloud architects; DevOps engineers; enterprise architects
	Existing Skills: Experience automating, developing and executing DevOps best-practices, providing solution architectures, and strategy for DevOps-adoption; ability to automate agile approaches for the cloud; background in software development, integration, and deployment; Infrastructure configuration and management; experience creating an infrastructure to help developers respond to user requests.
	Potential Training: Agile methodology, DevOps guidelines and standards
Phase(s)	Pre-Cloud Migration; Cloud Migration
Position Description Keyphrases	Architecture for continuous integration and deployment, and continuous monitoring; automation architect; experience serving as the engineer of complex technology implementations

<b>Facility Lead (if applicable)</b>	
Role	Individual(s) who are currently responsible for managing the on-premise data center operations and providing guidance on how to best utilize any remaining systems that do not move to the cloud. The lead will also manage on premise sites in conjunction with the cloud as part of an overall IT infrastructure approach.

Required Skills	Experience with data center optimization management (DCOM) tools; understanding of IT environments in the physical data center environment.
Reskilling	Titles: Facility engineer lead; data center IT operations manager
	Existing Skills: Property management experience; understanding of acquisitions
	Potential Training:
Phase(s)	Pre-Cloud Migration; Cloud Migration
Position Description Keyphrases	Facility maintenance and management; energy and power consumption experience

Procurement Lead (if applicable)	
Role	Individual(s) who are responsible for all procurement aspects of the cloud, including but not limited to procuring cloud services, migration services and/ or hardware necessary to adopt the cloud.
Required Skills	Contracting experience required; experience with cloud contracting preferred.
Desired Skills	Titles: Procurement officers; Federal Acquisition Services liaisons or POCs; Contracting Officer's Representatives (CORs)
Training and Resources	Existing Skills: Experience with navigating federal procurement processes, developing contracts, market research on cloud products
Agency Example(s)	Potential Training: <a href="#">Contracting (FAC-C) trainings</a> ; <a href="#">Contracting Officer's Representative (FAC-COR) trainings</a> ; <a href="#">Program and Project Managers (FAC-P/PM)</a>
Phase(s)	Cloud Migration; O&M
Position Description Keyphrases	Experience with Federal Acquisition Regulation; contract execution; DAWIA [Defense Acquisition Workforce Improvement Act]/FAC-C [ Federal Acquisition in Contracting Certification] level III in Contracting

## Compliance & Security Resources

Every Federal Information System needs an Authority to Operate (ATO) signed by an agency Authorizing Official. This requirement is not waived for cloud-based information systems.

Federal Information Security Management Act of 2002 (FISMA), along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a **risk-based policy for cost-effective security**. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) through Circular A-130, “Managing Federal Information as a Strategic Resource,” requires executive agencies within the federal government to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Periodically review the security controls in their systems
- Authorize system processing prior to operations and, periodically, thereafter

The FISMA publications are developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. The FISMA publications are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

### **Additional Security Requirements**

May be highly specialized - examples: Point of Sale (POS) or e-commerce transactions may/would require meeting Payment Card Industry (PCI) requirements. Healthcare / Medical data could/would require meeting Health Insurance Portability and Accountability Act (HIPAA) requirements. Educational records could/would require meeting Family Educational Rights and Privacy Act (FERPA) requirements.

### **Risk Management Framework Primer**

The Risk Management Framework (RMF) provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of systems into the mission and business processes of the organization. The diagram that follows provides a visual process flow for a system lifecycle, as well as the appropriate NIST reference documentation for each step.

#### [Prepare Step](#)

The preparation step of RMF is to ensure that the agency has the management structure in place to properly assign roles and responsibilities to the individuals who hold

security-related positions. This includes primary responsibilities such as the System Owner, Authorizing Official, and Information System Security Officer. It also ensures that there are policies and procedures in place for the NIST SP800-53 control families.

### [Categorize Step](#)

The categorization step should be completed before architecture and services are pursued. It is important to know the data that the system will be processing such that as the system is designed, all the required NIST SP800-53 baseline security controls are implemented as it is built, rather than attempting to tack them on at the end. Simply, the information system is categorized based on FIPS 199, NIST SP 800-60, and organizational guidance. The categorization decision is formally documented and is approved by the major stakeholders (ISSO, System Owner, Authorizing Official) of the system. At the end of this step, the system will be categorized as either “Low, Moderate, or High” based on NIST SP800-60 guidance. Additional categorization elements may include industry or application specific legislation, policies, directives, regulations, standards, and organizational mission/business/operational requirements.

### [Select Step](#)

The select step is often referred to as Control Tailoring step, as this is the step in which the NIST SP800-53 baseline security controls (for the determined system categorization) will be tailored for this, specific, system. If the ISSO, System Owner, or Authorizing Official desire, additional security controls can be specified for the system.

### Implement Step

The Implement Step is where the system is designed to adhere to the system categorization’s minimum security control baseline. This step includes the design, technology, and architecture as well as the policies and procedures required to ensure the system is designed using sound systems engineering practices and operated within the requirements for the system’s categorization. It is within this step that the system is developed and documented.

### Assess Step

The Assess Step reviews both the system documentation and the systems security control implementation effectiveness. The system is tested to confirm that the documented security control implementation meets the requirements for the system’s categorization, then confirms that the system is operating as documented. NIST SP800-53A provides the assessment rationale and procedures for completing an assessment. This assessment is traditionally conducting using an independent third party.

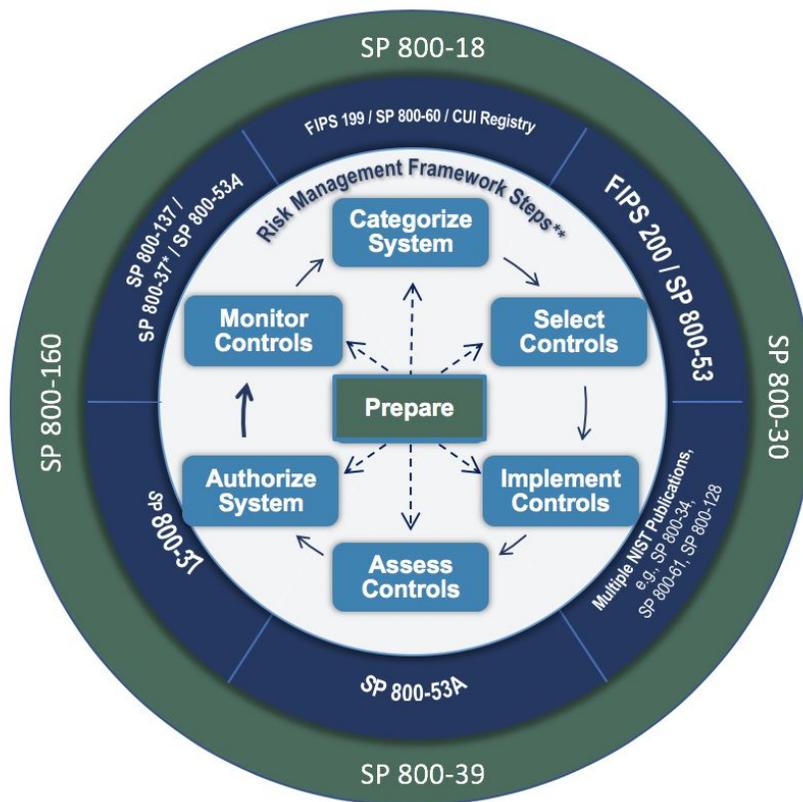
### [Authorize Step](#)

Security authorization is the official management decision given by a senior organizational official to authorize operation of a system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the

implementation of an agreed-upon set of security controls. The Authorizing Official (AO) may place limits or conditions upon the authorization as appropriate to ensure the system is operated in a manner that minimizes organizational risk. This authorization may have time limitations, such as a traditional three year period, or the system may be authorized to operated under an Ongoing Authorization model, provided that the Continuous Monitoring program is robust enough to support such.

Monitor Step

The Monitor Step is the continuous or periodic monitoring of the system to ensure that it continues to operate under the conditions specified within the authorization documentation (ATO). Monitoring includes the technology aspects of operating they system (log monitoring, intrusion detection, performance monitoring), as well as ensuring that that policies and procedures which apply to the system remain up to date, accurate, and applicable. The monitoring step also includes the change management process, ensuring that any and all changes to the system are documented and evaluated for security considerations prior to implementation.



**Figure 11: Risk Management Framework Steps**

## Governance Resources

The following is a list of the most common standards, best practices, and frameworks for CIOs.

- Control Objectives for Information and Related Technologies (COBIT)
- Application Services Library/Business Information Services Library (ASL/BiSL)
- Certified in the Governance of Enterprise IT (CGEIT)
- Project Management Body of Knowledge (PMBOK)
- Information Security Management (ISO) 17799
- Committee of Sponsoring Organizations (COSO)
- IT Governance for the Board, ISO 38500
- Information Technology Infrastructure Library (ITIL)
- Capability Maturity Model Integration (CMMI)
- Quality Management, Six Sigma
- Projects in Controlled Environments 2 (PRINCE2)
- Business Balanced Scorecard (BSC)
- IT Management, Lean IT
- Business Analysis Body of Knowledge (BABOK)

Below are some ideas and considerations to keep in mind when designing a tagging strategy that accommodates all of the various CSPs you may use:<sup>65</sup>

- Maximum Key Length (driven by GCP): 63 Characters
- Maximum Value Length (driven by GCP): 63 Characters
- Maximum # of Tags Per Resource (driven by Azure): 15 Tags
- Case Sensitive
- Keys and values can only contain lowercase letters, numeric characters, underscores, and dashes. International characters are allowed.
- Label keys must start with a lowercase letter and international characters are allowed.
- Label keys cannot be empty
- Tag names can't contain these characters: <, >, %, &, \, ?, /, @
- AWS-generated tag names and values are automatically assigned the aws: prefix, which you cannot assign. User-defined tag names have the prefix user: in the Cost Allocation Report.
- Use each key only once for each resource. If you attempt to use the same key twice on the same resource, your request will be rejected.
- You cannot tag a resource at the same time you create it. Tagging requires a separate action after the resource is created.

---

<sup>65</sup> <https://securityboulevard.com/2019/10/multi-cloud-tagging-strategies-for-the-win-2/>

- You cannot backdate the application of a tag. This means that tags only start appearing on your cost allocation report after you apply them, and do not appear on earlier reports.
- Tags applied to the resource group are not inherited by the resources in that resource group.
- Tags can't be applied to classic resources such as Cloud Services.